Ciberseguridad en el arbitraje

Yarubith Escobar Bastidas*

Principia No. Especial 1–2025 pp. 35-47

Resumen: La salvaguarda de la información es un tema crucial en el arbitraje internacional, y específicamente la ciberseguridad dentro de los procesos arbitrales es un asunto que ha cobrado gran relevancia en virtud de la creciente digitalización de los procedimientos y la sensibilidad de la información manejada. Los principios de privacidad, confidencialidad y flexibilidad presentes en el arbitraje lo hacen un blanco tentador para posibles ataques cibernéticos. En la actualidad, existen instrumentos jurídicos internacionales que han desarrollado el tema, así como también hay ejemplos de vulneración de la ciberseguridad en el arbitraje, los cuales serán abordados en este artículo.

Abstract: The safeguarding of information is a crucial issue in international arbitration, and specifically, cybersecurity within arbitral processes has become a matter of great relevance due to the increasing digitalization of proceedings and the sensitivity of the information handled. The principles of privacy, confidentiality, and flexibility inherent in arbitration make it an attractive target for potential cyberattacks. Currently, there are international legal instruments that address this issue, as well as cases of cybersecurity breaches in arbitration, which will be discussed in this article.

Palabras Claves: Ciberseguridad | Arbitraje internacional | Protección de la información | Digitalización | Confidencialidad | Flexibilidad | Ataques cibernéticos

Keywords: Cybersecurity | International arbitration | Information protection | Digitalization | Confidentiality | Flexibility | Cyberattacks

* Certificada por Harvard University en Cybersecurity: Managing Risk in the Information Age. LL.M en Resolución de Disputas en la University of Missouri-Columbia. MBA (International Business) por la San Ignacio University de Miami, mención Cum Laude. Certificada por el Programa Avanzado de Estudios en Arbitraje de la Universidad Monteávila. Abogada y Licenciada en Estudios Internacionales por la Universidad Central de Venezuela.

Sumario: I. Introducción, II. Principios claves en el Arbitraje y su relación con la Ciberseguridad, III. Instrumentos Jurídicos Internacionales sobre Ciberseguridad en el Arbitraje, IV. Casos de Vulneración de la Ciberseguridad en el Arbitraje, V. Consecuencias de un Ciberataque en el Arbitraje Internacional, VI. Medidas para Mitigar Riesgos Cibernéticos en el Arbitraje, VII. Conclusiones

I. Introducción

El arbitraje internacional es un medio sobresaliente para la resolución alternativa de disputas en el contexto global, y en contraposición a los tribunales regulares o tradicionales, el arbitraje incorpora como parte de su naturaleza jurídica principios básicos como la flexibilidad y la confidencialidad que hacen muy atractivo el uso de este mecanismo En escenarios donde las partes en conflicto pueden pertenecer a diferentes jurisdicciones, el arbitraje proporciona imparcialidad y eficiencia para resolver disputas de naturaleza comercial, laboral, deportiva, de inversiones, entre otras. El arbitraje se rige por la voluntad de las partes y el procedimiento se lleva a cabo bajo reglas específicas convenidas de mutuo acuerdo e incluye la elección de los árbitros y la aplicabilidad de tratados internacionales[1].

En la actualidad, el arbitraje internacional ha sufrido una evolución transcendental debido al uso de las tecnologías de la información y la comunicación, así como la digitalización de los procedimientos. Cada vez es más común que las fases del procedimiento arbitral como la presentación de memoriales, de pruebas e incluso las audiencias se lleven a cabo en entornos virtuales, mediante el uso de plataformas digitales. Toda esta transformación electrónica se ha traducido en mayor eficiencia, accesibilidad para las partes en conflicto y hasta en reducción de costos[2].

No obstante, el uso de tecnologías en el arbitraje también ha traído consigo desafíos importantes en cuanto a la seguridad de la información. El uso de redes digitales y las plataformas de almacenamiento en la nube son herramientas que aumentan la exposición a ciberataques y a posibles filtraciones de la información, poniendo en riesgo la integridad del proceso y el principio de confidencialidad.

De esta forma, la ciberseguridad se erige como una preocupación relevante dentro del arbitraje internacional, debido a

[1] M. Estévez, "Ciberseguridad en los procesos de arbitraje internacional," *Izertis* (2024), https://www.izertis.com/es/-/blog/ciberseguridad-procesos-arbitraje-internacional

[2] Cuando se menciona que la transformación digital del arbitraje ha traído consigo ventajas como mayor eficiencia, accesibilidad para las partes en conflicto y reducción de costos, se hace referencia a que por ejemplo ha habido reducción en la impresión de enormes documentos físicos, quizá ya no es necesario trasladarse de un país s otro para la celebración de las audiencias, sino que se puede participar de manera virtual a través de plataformas especializadas, entre otros ejemplos.

que la información que se maneja en estos procedimientos suele ser muy sensible[3]. Y cuando se habla de la sensibilidad de la información en el arbitraje internacional se habla de documentos relacionados con disputas comerciales, datos financieros, contratos, secretos industriales, decisiones arbitrales no publicadas, datos personales de las partes involucradas, pruebas y testimonios confidenciales, estrategias de negociación, etc. Este tipo de información sumamente relevante puede ser objeto de ataques por parte de hackers, gobiernos, competidores desleales, entre otros sujetos interesados en obtener acceso a dicha información estratégica.

Una falla en la ciberseguridad dentro de un procedimiento arbitral puede tener consecuencias gravísimas que van desde poner en riesgo la privacidad de las partes hasta comprometer la validez del laudo, es por lo que organizaciones internacionales relacionadas al mundo del arbitraje han desarrollado algunos instrumentos jurídicos con recomendaciones y protocolos para fortalecer la seguridad de la información en esta era digital.

Este artículo explora de manera general los principales marcos normativos que abordan la ciberseguridad en el arbitraje internacional, así como algunos casos relevantes de vulneración y las consecuencias de estos incidentes en los procedimientos arbitrales.

II. Principios claves en el Arbitraje y su relación con la Ciberseguridad

Entre los principios fundamentales del arbitraje destacan la confidencialidad y la flexibilidad, elementos estos que separan al arbitraje de los litigios judiciales, pero que por otro lado lo hacen vulnerable dentro de un entorno tecnológico. En este orden de ideas, la sensibilidad política y comercial de las disputas arbitrales, que a menudo son confidenciales gracias a esa flexibilidad arbitral, las convierte en un blanco atractivo para los hackers[4].

La confidencialidad es un elemento central dentro de los procesos de arbitraje, ya que es el que garantiza que la información dentro del procedimiento (memoriales, pruebas, testimonios, el laudo, etc.) sea reservada y su acceso restringido a las partes involucradas y al tribunal arbitral. Es necesario mencionar que el nivel de confidencialidad varia de arbi-

[3] Frecuentemente la batería de información a la cual se tiene acceso durante un procedimiento de arbitraje internacional, es altamente sensible en virtud de la naturaleza del conflicto y a los intereses en juego. Por ejemplo, la filtración por un ciberataque de secretos comerciales y propiedad intelectual en disputas relacionadas con patentes o formulas comerciales. Otro ejemplo es el caso de la filtración de datos financieros y bancarios donde se podría exponer la estrategia financiera de un fondo de inversión o su estructura fiscal.
[4] J. Choong, V. Sinha, S. Klot, y O. André, "Data Protection and Cybersecurity in International Arbitration Remain in the Spotlight," *Freshfields Bruckhaus Deringer* (2023), https://www.freshfields.com/en-gb/our-thinking/campaigns/international-arbitration-in-2023/data-protection-and-cybersecurity-in-international-arbitration-remain-in-the-spotlight/

traje a arbitraje y va a depender de lo que las partes acuerden al respecto, habrá arbitrajes más abiertos a publicar información relevante y habrá arbitrajes a puerta cerrada[5]. Cualquier brecha en la ciberseguridad del arbitraje puede traducirse en la exposición pública de información sensible catalogada como confidencial por las partes.

Otro principio medular del arbitraje es su flexibilidad, el cual permite que las partes adapten el procedimiento a sus necesidades, y sin duda la digitalización de los procedimientos ha profundizado esa flexibilidad y en virtud de ello ahora vemos audiencias virtuales, firma electrónica de documentos, almacenamiento en la nube, etc.

Todas estas innovaciones tecnológicas han traído consigo riesgos significativos en cuanto a la seguridad digital de la información arbitral se refiere. Por ejemplo, la carencia de uniformidad en los estándares de protección de datos y la variedad de plataformas digitales que son utilizadas hacen que la generación de brechas de seguridad sea cada vez más frecuente[6].

En otras palabras, el interés de terceros, ajenos o participantes, en tener acceso a la información y datos relacionados con el arbitraje hace que los activos tecnológicos mediante los cuales se almacena, gestionan y comunica dicha información sea un blanco atractivo para los ciberdelincuentes[7].

III. Instrumentos Jurídicos Internacionales sobre Ciberseguridad en el Arbitraje

Afortunadamente hoy día la comunidad internacional cuanta con algunos instrumentos jurídicos internacionales que plantean directrices orientadas a proteger la información sensible que se maneja en los arbitrajes, así como prevenir ataques y garantizar la confidencialidad y la integridad de dichos procedimientos. Veamos de que se tratan algunos de estos instrumentos:

- **Directrices de Ciberseguridad de la IBA[8]:** Estas directrices fueron adoptadas en el 2018 por la *International Bar Association* y las mismas están orientadas a proponer las mejores prácticas para que los abogados se resguarden de las violaciones de seguridad de los da-

[5] Estévez, "Ciberseguridad en los procesos de arbitraje internacional."
[6] Por ejemplo, cuando una audiencia arbitral se lleva a cabo mediante una plataforma virtual de videoconferencias, y la misma no posee un cifrado robusto y adecuado, existe el riesgo de que un tercero pueda interceptar la transmisión y obtener acceso no autorizado a las deliberaciones del caso. Hay un término para conceptualizar esto y es el *Zoombombing*, el cual se define como es una intrusión, indeseada y perturbadora, por hackers de Internet o terceros no autorizados, en una videoconferencia.
[7] Estévez, "Ciberseguridad en los procesos de arbitraje internacional."
[8] International Bar Association, *IBA Cybersecurity Guidelines* (International Bar Association, 2018), https://www.ibanet.org/MediaHandler?id=2F9FA5D6-6E9D-413C-AF80-681BAFD300B0

tos e información y la posible responsabilidad correspondiente[9].

- **Protocolo ICCA – NYC Bar CPR sobre Ciberseguridad en el Arbitraje Internacional:** Este protocolo fue publicado en el 2019 y tuvo una actualización el 2022 y es fruto de un esfuerzo conjunto del Consejo Internacional de Arbitraje Comercial (ICCA), el Colegio de Abogados de la Ciudad de Nueva York y el Instituto Internacional para la Prevención y Resolución de Conflictos (CPR)[10]. Dicho instrumento provee con un marco general para que las partes acuerden medidas pertinentes de ciberseguridad para la protección de sus arbitrajes. Algunas de estas posibles medidas son el cifrado, los controles de acceso, entre otros. Este protocolo aborda cuestiones de seguridad de los datos y de la información que podrían ser incorporados a los acuerdos arbitrales, órdenes del día, ordenes procesales, etc., así como una guía para notificar y gestionar violaciones de ciberseguridad[11].

- **La Hoja de Ruta para la Protección de Datos en el Arbitraje Internacional:** También del 2022, fue elaborada por la IBA (*International Bar Association)* y la CPA (Corte Permanente de Arbitraje) con el objetivo principal de identificar y abordar de manera eficaz y eficiente las cuestiones relativas a la protección de datos en el arbitraje, incluidos aquellos almacenados de forma digital[12].

- **Reglamento General de Protección de Datos (RGPD) de la Unión Europea:** Este instrumento es aplicado a cualquier institución que procese "datos personales" de ciudadanos de la Unión Europea, independientemente de su ubicación geográfica. En el marco de los arbitrajes, los "datos personales" pueden incluir nombres, direcciones, detalles financieros, información de contactos, detalles sociales, etc. En este sentido, de acuerdo con este instrumento jurídico, los abogados deben obtener consentimiento explicito tanto de testigos como de expertos antes de procesar sus "datos personales". Este reglamento, además restringe la transferencia de "datos personales" a países fuera de la jurisdicción de la Unión Europea que no posean un nivel de protección de datos correcto. En

[9] D. Nikolić y S. Supper, "Cybersecurity in International Arbitration: On the Road towards Green Flags," *Schoenherr Attorneys at Law* (2024), https://www.schoenherr.eu/content/cybersecurity-in-international-arbitration-on-the-road-towards-green-flag
[10] Nikolić y Supper, "Cybersecurity in International Arbitration."
[11] Choong et al., "Data Protection and Cybersecurity in International Arbitration."
[12] Nikolić y Supper, "Cybersecurity in International Arbitration."

un arbitraje internacional, esto resulta especialmente relevante, sobre todo en la celebración de audiencias virtuales con partes localizadas en diferentes jurisdicciones[13].

- También los centros de arbitraje han ido creando sus propios mecanismos de protección de datos y ciberseguridad a través de recomendaciones e inclusos la imposición de obligaciones a los árbitros de discutir cuestiones relacionadas con la protección de los datos y si lo consideran necesario, emitir decisiones al respecto[14]. Ejemplo de ello es el **LCIA** ***London Court of International Arbitration*****)** cuyo reglamento de arbitraje obliga al tribunal y a las partes a considerar las cuestiones de seguridad de la información desde el principio del procedimiento e incluir dichas consideraciones en la conferencia procesal inicial. Otro ejemplo, lo constituye el **Reglamento Suizo** ***(Swiss Rules of International Arbitration*** del ***Swiss Arbitration Centre)*** el cual promueve el uso de plataformas digitales seguras y fomenta que las partes discutan *at initio* medidas específicas de seguridad informática para la protección de los datos. Por otro lado, el **SIAC** ***(Singapore International Arbitration Centre)*** emitió durante y después del Covid-19 protocolos y guías para llevar a cabo las audiencias virtuales haciendo énfasis en el uso de plataformas seguras, el uso de fuertes controles de acceso y privacidad robusta[15]. También el **VIAC** ***(Vienna International Arbitral Centre)*** publico directrices sobre las audiencias online recomendando medidas sobre la autenticación de los participantes del arbitraje y la prevención de grabaciones no autorizadas.

Se observa entonces como de manera directa e incluso de manera indirecta, la comunidad arbitral internacional cuenta con instrumentos jurídicos relativos al tema de la protección de la información en esta era digital, demostrando así la preocupación que existe al respecto.

IV. Casos de Vulneración de la Ciberseguridad en el Arbitraje

La confidencialidad es uno de los principios por los cuales el arbitraje es tan popular como medio alternativo de resolu-

[13] The Impact Lawyers, "COVID-19 y la protección de datos en el arbitraje internacional," *The Impact Lawyers* (2021), https://theimpactlawyers.com/es/articulos/covid-19-y-la-proteccion-de-datos-en-el-arbitraje-internacional

[14] Nikolić y Supper, "Cybersecurity in International Arbitration."

[15] Shaun Lee y Low Zhe Ning, "SIAC Congress Recap: This House Believes that Virtual Hearings Are Just as Effective as In-Person Hearings," *Kluwer Arbitration Blog*, 4 de septiembre de 2020, https://arbitrationblog.kluwerarbitration.com/2020/09/04/siac-congress-recap-this-house-believes-that-virtual-hearings-are-just-as-effective-as-in-person-hearings/

ción de controversias. Sin embargo, la confidencialidad se ha visto comprometida en algunas ocasiones debido a brechas en la seguridad de la información y a las actuaciones de actores involucrados en el arbitraje (despachos de abogados, empresas, Estados, etc.)[16]. Veamos algunos casos relevantes:

1. **Ataque al sitio web de la Corte Permanente de Arbitraje (CPA) (China vs. Filipinas, 2015):** Este hackeo se produjo en el momento de la celebración de una audiencia entre China y Filipinas en un caso relacionado con una disputa de tipo fronteriza y marítima. Y como consecuencia de ello, los datos personales de todo aquel involucrado en este caso quedaron expuestos[17]. Básicamente lo ocurrido este en caso concreto, fue la instalación de un *malware*[18] en la parte o sección de la página web de la CPA dedicada a esa disputa, pero que además contenía información relevante de otra docena de casos, lo que llevo a la desconexión de la página web por motivos de seguridad de los datos[19]. Hay que destacar que este ataque fue atribuido a China, y el mismo permitió que cualquier persona que visitara ese sitio web, su equipo quedaba infectado por un programa malicioso que le daba la oportunidad a China de tener acceso a toda la información del computador desde el cual se accedía. De esta forma China pudo obtener los nombres de los actores que formaban parte y seguían este caso y así anticipar su postura ante la CPA[20].
2. ***Gela Mikadze et al. v. Ras Al Khaimah Investment Authority et al.*, Cámara de Comercio de Estocolmo (SCC):** En este caso, una de las partes dio inicio al procedimiento de anulación de laudo, alegando ante los tribunales suecos que hubo violación al debido proceso porque se dio un pirateo de información clasificada como confidencial, señalando que dicho hecho ocurrió por instrucciones de la parte contraria[21].
3. ***Caratube International Oil Company LLP y Devincci Salah Hou-***

[16] Javier Fernández-Samaniego, Gonzalo Hierro Viéitez, y Yaiza Araque Moreno, "Ciberseguridad en el Arbitraje Internacional: Un Desafío Inaplazable," *THEMIS Revista de Derecho*, no. 79 (2021): 549, https://revistas.pucp.edu.pe/index.php/themis/article/view/23502/22480

[17] Fernández-Samaniego, Hierro Viéitez y Araque Moreno, "Ciberseguridad en el Arbitraje Internacional," 549.

[18] Según la pagina web de McAfee un *malware* es "un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras." https://www.mcafee.com/esmx/antivirus/malware.html#:~:text=%C2%BFQu%C3%A9%20es%20malware?,comprometida%20se%20ha%20vuelto%20ilimitada.

[19] Nikolić y Supper, "Cybersecurity in International Arbitration."

[20] Estévez, "Ciberseguridad en los procesos de arbitraje internacional."

[21] Nikolić y Supper, "Cybersecurity in International Arbitration."

rani c. Kazajistán: Este es un caso de arbitraje internacional de inversiones, donde se le presentaron al tribunal arbitral documentos filtrados que fueron obtenidos a través de un hackeo de los sistemas informáticos del gobierno de Kazajistán y que fueron usados por la parte demandante en el proceso arbitral[22]. Este caso involucro al bufete internacional Curtis, Mallet-Prevost, Colt quienes accionaron en nombre de Kazajistán, tras tener conocimiento que algunas cuentas de correo electrónico y computadoras de diversos funcionarios públicos del gobierno de este país habían sido hackeadas durante el tiempo que ese bufete asesoraba a Kazajistán en relación con un acuerdo para desarrollar un yacimiento de petróleo y gas[23].

4. ***ConocoPhillips contra Venezuela:*** Este es otro caso de arbitraje internacional de inversiones donde se presentaron documentos contentivos de comunicaciones entre funcionarios vinculados con el arbitraje que posteriormente aparecieron en *WikiLeaks*[24].

Estos son solo algunos ejemplos que muestran que los ciberataques en los procedimientos arbitrales son amenazas reales.

V. Consecuencias de un Ciberataque en el Arbitraje Internacional

Una falla en la ciberseguridad dentro de un arbitraje internacional puede representar una amenaza a la integridad y legitimidad del procedimiento. El hecho de que cada vez más los arbitrajes se desarrollen en entornos digitales hace que las posibles consecuencias de un ciberataque u otra falla en la seguridad de la información puedan llegar a ser de amplio alcance y bastante significativas. Veamos algunos de los impactos más importantes:

Una de las principales consecuencias de la vulneración en la ciberseguridad en el contexto de un arbitraje internacional es la ruptura del principio de confidencialidad y por lo tanto de la integridad de la información y de los datos manejados dentro del procedimiento. La fuga de información en un arbitraje puede ser utilizada como un arma de negociación que puede perjudicar las posturas de las partes en conflicto y alterar el curso del proceso. La filtración o eliminación de información relevante como comunicaciones entre las partes, emails, pruebas, borradores de los memoriales o del laudo pueden incidir directamente en la equidad del procedimiento y debilitar la confianza en este mecanismo alternativo de resolución de controversias.

[22] Nikolić y Supper, "Cybersecurity in International Arbitration."
[23] Fernández-Samaniego, Hierro Viéitez y Araque Moreno, "Ciberseguridad en el Arbitraje Internacional," 549.
[24] Nikolić y Supper, "Cybersecurity in International Arbitration."

La confidencialidad en el arbitraje internacional requiere de la ciberseguridad[25]. En esta época de procedimientos arbitrales verdes (sin papel), pero con una enorme cantidad de datos electrónicos, estos pueden estar expuestos a accesos no autorizados sino se implementan medidas de ciberseguridad robustas.

Es importante mencionar que el impacto de la filtración de información en un arbitraje no afecta solo a las partes en conflicto, sino que puede potencialmente afectar a terceros involucrados como empleados, clientes, competidores, etc. Por ejemplo, la divulgación de información relativa a los pronósticos financieros, propiedad intelectual, planes de negocios, etc., puede ser usada negativamente en contra de las empresas parte del conflicto, afectando el valor de sus acciones, o su posición en el mercando, pérdidas económicas e incluso afectar su reputación[26].

Como se mencionó *ut supra,* pueden darse daños reputacionales como consecuencia de fallas de ciberseguridad en un arbitraje, y si se percibe que dichas fallas fueron consecuencia de no tomar las medidas necesarias para la protección de la información, estos daños pueden extenderse también a los abogados, a los peritos y a los árbitros. Ahora bien, si hablamos de arbitrajes internacionales de inversión, hay que tener en cuenta que la fuga de información relevante puede llegar a generar crisis diplomáticas y presiones políticas.

En este sentido, también podría darse el escenario de la divulgación no autorizada de datos personales por ejemplo de los testigos y expertos y esto puede afectarlos en su fuero privado.

Otra consecuencia grave de un ciberataque en un procedimiento arbitral es el impacto en la validez y ejecución del laudo. Los laudos arbitrales son decisiones vinculantes entre las partes y su validez está sujeta a que todo el procedimiento se haya llevado a cabo con transparencia, rectitud y sin vulneraciones; y un ataque cibernético que modifique o manipule las pruebas, las comunicaciones o algún dato relevante dentro del proceso podría potencialmente dar lugar a impugnaciones sobre el laudo. En este escenario, algunas de las partes podrían argumentar que no se respectaron las garantías fundamentales, podrían darse alegaciones de corrupción, falta de imparcialidad, violaciones al debido proceso, etc., y todo esto puede dar lugar a que se intenten acciones de nulidad contra el laudo o su no reconocimiento.

En definitiva, las consecuencias de fallas en la ciberseguridad en el arbitraje internacional variaran de acuerdo con las circunstancias particulares del caso concreto, pero en términos generales podría haber aumento del costo del arbitraje, pérdida económica para la parte cuya in-

[25] Nikolić y Supper, "Cybersecurity in International Arbitration."
[26] Nikolić y Supper, "Cybersecurity in International Arbitration."

formación fue vulnerada, daños reputacionales, retrasos en el procedimiento, cuestionamientos de imparcialidad de los árbitros, desacuerdos en las medidas a tomar para evitar más fallas, posible responsabilidad contractual, cobertura mediática adversa, etc[27].

VI. Medidas para Mitigar Riesgos Cibernéticos en el Arbitraje

Ante las graves consecuencias que puede potencialmente generar la debilidad en la seguridad de la información dentro de un procedimiento de arbitraje internacional en este creciente era digital, resulta imperativo tomar medidas preventivas e implementar protocolos robustos de ciberseguridad orientados a la mitigación del riesgo.

La buena noticia es que la comunidad arbitral internacional es consciente de los grandes desafíos de ciberseguridad que existen hoy en día. En otras palabras, la ciberseguridad en el arbitraje internacional es tarea de todos los actores involucrados (partes, abogados, tribunales arbitrales, centros de arbitraje, peritos, expertos, terceros financiadores, etc.) y todos deben asumir su cuota de responsabilidad en la protección de los datos y de las comunicaciones.

Existe consenso en que la responsabilidad compartida, la responsabilidad activa y las medidas preventivas son medulares para garantizar la protección de los datos digitales en los procedimientos arbitrales[28].

Como ya se describió en la parte III de este artículo titulada "Instrumentos Jurídicos Internacionales sobre Ciberseguridad en el Arbitraje" ha habido un esfuerzo por parte de la comunidad arbitral internacional en crear y poner a disposición de los usuarios del arbitraje documentos contentivos de buenas prácticas tendentes a proteger a los arbitrajes de posibles ciberataques.

En este sentido, y más allá de los instrumentos jurídicos, hojas de ruta, recomendaciones, directrices, protocolos, que ya existen y que seguramente se continuaran elaborando en el concierto del arbitraje internacional, existen medidas preventivas que se pueden implementar incluso antes de que comience el arbitraje. Por ejemplo, las empresas pueden tomar acciones precautorias como realizar evaluaciones preliminares de riesgo para identificar previamente los documentos confidenciales y los datos sensibles que serán introducidos en el procedimiento arbitral y de acuerdo con el resultado crear protocolos internos de seguridad e incluso crear canales seguros para la comunicación relacionada con el arbitraje, crear copias de seguridad, implementar antivirus en sus sistemas informáticos, si usas memorias USB estas

[27] Anastasia Tzevelekou, "Cybersecurity in International Arbitration," *International Arbitration Attorney*, 30 de enero de 2020, https://www.international-arbitration-attorney.com/cybersecurity-in-international-arbitration/

[28] Nikolić y Supper, "Cybersecurity in International Arbitration."

deben estar cifradas y el acceso a los documentos digitales debe estar protegido por contraseñas complejas o autenticación multifactorial[29].

La capacitación continua también es otro elemento para tomar en cuanta. Los actores en el arbitraje deben estar formados sobre los temas de seguridad de la información y su medular importancia para la integridad del arbitraje. Además de la capacitación en el tema y la promoción de la cultura de seguridad, también se podría exigir la destrucción de ciertos documentos una vez concluya el arbitraje[30]. En este sentido, es importante entender que le prevención en temas de seguridad de la información depende en gran medida del comportamiento humano, es por lo que todos los actores involucrados en un procedimiento arbitral deberían estar al tanto de asuntos de ciberseguridad como el manejo adecuado de contraseñas, reconocimiento de correos maliciosos, procedimientos en caso de sospecha de perdida de la información o intrusión, etc.

Por otro lado, los centros administradores de arbitrajes también tienen un papel protagónico en lo que a ciberseguridad se refiere, y sobre ellos recae proveer y asegurarse de que los tribunales arbitrales usen plataformas fuertes con cifrados de extremo a extremo, sistemas de autenticación multifactorial y almacenamiento en la nube con estándares internacionales de seguridad como la ISO/IEC 27001. Esta certificación es un estándar usado globalmente que muestra que una organización implementa buenas prácticas de seguridad informática y es confiable[31]. En este orden de ideas, las instituciones arbitrales pueden desplegar estrategias centralizadas de ciberseguridad en aras de mitigar la sofisticación de los ataques cibernéticos actuales[32].

Otra medida de mitigación de riesgos en el arbitraje internacional que puede ser implementada son los acuerdos entre las partes sobre seguridad digital. Es recomendable que las partes establezcan por consenso cláusulas sobre ciberseguridad en sus reglas de procedimiento, como por ejemplo protocolos para el intercambio de documentos, reglas sobre el uso de dispositivos personales, mecanismos de respaldo de información, entre otros, en aras de fortalecer la transparencia y anticiparse a escenarios de contingencia ante posibles incidentes en cuanto a la seguridad de la información.

VII. Conclusiones

La ciberseguridad en el arbitraje internacional se erige como un tema medianamente novedoso, cuya importancia real se intensificó durante el periodo del Covid-19, a raíz de la necesidad de celebrar

[29] Nikolić y Supper, "Cybersecurity in International Arbitration."
[30] Nikolić y Supper, "Cybersecurity in International Arbitration."
[31] Estévez, "Ciberseguridad en los procesos de arbitraje internacional."
[32] Tzevelekou, "Cybersecurity in International Arbitration."

las audiencias virtualmente. Pero la realidad ha demostrado que toda esta digitalización en los procedimientos de arbitraje, especialmente en el arbitraje internacional, llegó para quedarse. Sin embargo, más allá de los múltiples beneficios de la virtualidad, han surgido desafíos en cuanto a la seguridad de la información que han puesto en alerta a la comunidad arbitral y que la han llevado a tomar medidas al respecto.

Como se observó en el desarrollo de este artículo existe una variedad de instrumentos jurídicos internacionales que ofrecen marcos orientativos para enfrentar de la mejor manera posible y con uniformidad estos desafíos, ofreciendo soluciones y promoviendo mejores prácticas como estrategias de mitigación.

Por otro lado, existen precedentes de vulneración y fallas en la ciberseguridad en procedimientos de arbitraje que demuestran que el riesgo no es hipotético, sino real. Las posibles consecuencias de un ciberataque van a depender del caso concreto, pero en términos generales se puede comprometer la validez de laudo, o dañar la reputación de las partes o actores del arbitraje, así como el incremento en los costos del procedimiento debido al retraso procesal que se puede causar, y finalmente se podría ver socavada la legitimidad del proceso.

En este sentido, se hace necesario implementar medidas preventivas como la adopción de plataformas tecnológicas robustas, y la participación activa de los involucrados en el arbitraje para garantizar la eficacia, la confianza, la confidencialidad, y la sostenibilidad del arbitraje como medio alternativo de resolución de conflictos en este era digital.

En este orden de ideas, resulta oportuno recomendar que las partes incluyan clausulas específicas sobre la seguridad digital en sus órdenes procesales que de manera consensuada ayuden a blindar y proteger el procedimiento. Otra recomendación tiene que ver con la formación continua en temas de protección de datos y el manejo de plataformas tecnológicas, la cual debería ser impartida a todos los actores involucrados en el arbitraje.

En cuanto a futuras líneas de investigación que se pueden desprender de este importante tema, resulta necesario profundizar en el impacto jurídico de las fallas de ciberseguridad en la validez del laudo arbitral, así como la responsabilidad de los actores involucrados. También sería pertinente ver como la inteligencia artificial y el almacenamiento en la nube afectan la confidencialidad del arbitraje y su consecuente eficacia. Por otro lado, sería interesante que los más importantes centros de arbitraje del mundo armonizaran estándares internacionales de ciberseguridad.

Para finalizar, es importante resaltar que la ciberseguridad no es un fin en sí mismo, sino es el medio para proteger el proceso arbitral en esta era digital. Es necesario prevenir, pero sin olvidar que

la figura protagónica es el arbitraje, y hacia su integridad es a donde deben dirigirse todos los esfuerzos. Por lo tanto, la evaluación de los costos económicos de la implementación de medidas de ciberseguridad es sin duda un tema que debe ser evaluado.