Thomson Reuters Data Security Addendum

Version 2.0

Last Modified: November 3, 2023

This Data Security Addendum (the "***Addendum***") amends the Agreement between Thomson Reuters and Customer and sets out the obligations of both parties regarding the security of Your Data in connection with the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum will take precedence only with respect to the security of Your Data. Customer will be the same as "Customer", "Client", or "you"; and Thomson Reuters will mean the same as "us", "we", "TR" or "Thomson Reuters", as the terms may be used in the Agreement.

1. INFORMATION SECURITY PROGRAM

1.1 Thomson Reuters will maintain an information security program that adopts the International Organization for Standardization (ISO/IEC 27002:2013) and/or the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The program will include, but is not limited to, the following components:

(i) Information security policy framework;

(ii) Program documentation;

(iii) Auditable controls;

(iv) Compliance records; and

(v) Appointed security officer and information security personnel.

1.2 Thomson Reuters will establish and maintain information security policies designed to protect the confidentiality and integrity of Your Data hosted in the Services, which will include the following:

(i) Policies to restrict access to Your Data only to authorized Thomson Reuters personnel and subcontractors;

(ii) Policies requiring the use of user ID's, passwords, and multi-factor authentication to access Your Data;

(iii) Policies requiring connections to the internet to have commercially reasonable controls to help detect and terminate unauthorized activity prior to the firewall maintained by Thomson Reuters;

(iv) Policies requiring performance of periodic vulnerability assessments;

(v) Policies for the use of anti-malware and patch management controls to help protect against virus or malware infection and exploitation of security vulnerabilities; and

(vi) Policies and standards for the use of auditable controls that record and monitor activity.

1.3 Thomson Reuters will train and communicate to Thomson Reuters personnel its defined information security principles and information

Adenda de Seguridad de Datos de Thomson Reuters

Versión 2.0

Última Modificación: 03 de noviembre de 2023

Esta Adenda de Seguridad de Datos (la "***Adenda***") modifica el Contrato entre Thomson Reuters y el Cliente y establece las obligaciones de ambas partes respecto de la seguridad de Sus Datos en relación con el Contrato. En caso de conflicto entre los términos y condiciones de esta Adenda y el Contrato, prevalecerán los términos y condiciones de esta Adenda únicamente respecto de la seguridad de Sus Datos. Cliente será lo mismo que "Cliente" o "usted"; y Thomson Reuters significará lo mismo que "nosotros", "TR" o "Thomson Reuters", según se utilicen los términos en el Contrato.

1. PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

1.1 Thomson Reuters mantendrá un programa de seguridad de la información que adopta la Organización Internacional de Normalización (ISO/IEC 27002:2013) y/o el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF). El programa incluirá, pero no se limitará a, los siguientes componentes:

(i) Marco de políticas de seguridad de la información;

(ii) Documentación del Programa;

(iii) Controles auditables;

(iv) Registros de cumplimiento; y

(v) Oficial de seguridad designado y personal de seguridad de la información.

1.2 Thomson Reuters establecerá y mantendrá políticas de seguridad de la información diseñadas para proteger la confidencialidad e integridad de Sus Datos alojados en los Servicios, que incluirán lo siguiente:

(i) Políticas para restringir el acceso a Sus Datos solo al personal y subcontratistas autorizados de Thomson Reuters;

(ii) Políticas que requieren el uso de ID´s de usuario, contraseñas, y autenticación multi factor para acceder a Sus Datos;

(iii) Políticas que requieren que las conexiones a Internet tengan controles comercialmente razonables para ayudar a detectar y terminar la actividad no autorizada antes del firewall mantenido por Thomson Reuters;

(iv) Políticas que requieren la realización de evaluaciones periódicas de vulnerabilidad;

(v) Políticas para el uso de controles de administración de parches y antimalware para ayudar a proteger contra infecciones de virus o malware y la explotación de vulnerabilidades de seguridad; y

(vi) Políticas y estándares para el uso de controles auditables que registran y monitorean la actividad.

1.3 Thomson Reuters capacitará y comunicará al personal de Thomson Reuters sus principios definidos de seguridad de la información y las

security policies and standards in accordance with the following:

(i) Applicable Thomson Reuters personnel will be required to take training, both at hire and on a regular basis, in information security practices and the correct use of information processing facilities to minimize possible security threats;

(ii) Applicable Thomson Reuters personnel will be instructed to report any observed or suspected threats, vulnerabilities, or incidents to our Security Operations Center; and

(iii) Thomson Reuters information security personnel will be made aware of reported information security threats and concerns and will support the Thomson Reuters information security policy in the course of their normal work.

1.4 Thomson Reuters will be responsible for its personnel's compliance with the terms of the Agreement and with Thomson Reuters standard policies and procedures. Thomson Reuters will maintain a disciplinary process to address any unauthorized access, use, or disclosure of Your Data by any Thomson Reuters personnel.

1.5 Thomson Reuters will maintain a formal plan for incident response to promptly respond to suspected or confirmed breaches of Your Data in accordance with regulatory and legal obligations.

1.6 Thomson Reuters policy with respect to user IDs and passwords for Thomson Reuters personnel accessing Thomson Reuters systems includes, but is not limited to, the following components:

(i) Each user has a unique account identifier or user ID;

(ii) Each user ID or account is assigned a password;

(iii) User IDs are added, modified, and deleted in accordance with Thomson Reuters approved account management processes;

(iv) Verification of user identify before password resets;

(v) Passwords must conform to defined criteria that include length, complexity requirements and limitations on reuse;

(vi) User IDs, passwords and tokens are not shared or used by anyone other than the user to whom it was assigned;

(vii) Temporary or default passwords are set to unique values and changed after first use;

(viii) User ID password changes are required at least every ninety (90) days;

(ix) Failed and repeated access attempts are locked for a reasonable and appropriate duration;

(x) Idle sessions are locked after a commercially reasonable period of time; and

(xi) User IDs are disabled after personnel termination.

políticas y estándares de seguridad de la información de acuerdo con lo siguiente:

(i) Se requerirá que el personal correspondiente de Thomson Reuters reciba capacitación, tanto en el momento de la contratación como de manera regular, en prácticas de seguridad de la información y el uso correcto de las instalaciones de procesamiento de información para minimizar las posibles amenazas a la seguridad;

(ii) El personal correspondiente de Thomson Reuters recibirá instrucciones para informar cualquier amenaza, vulnerabilidad o incidente observado o sospechado a nuestro Centro de Operaciones de Seguridad; y

(iii) El personal de seguridad de la información de Thomson Reuters estará al tanto de las amenazas y preocupaciones de seguridad de la información informadas y apoyará la política de seguridad de la información de Thomson Reuters en el curso de su trabajo normal.

1.4 Thomson Reuters será responsable del cumplimiento de su personal de los términos del Contrato y de las políticas y procedimientos estándar de Thomson Reuters. Thomson Reuters mantendrá un proceso disciplinario para atender cualquier acceso, uso, o divulgación no autorizada de Sus Datos por parte de cualquier personal de Thomson Reuters.

1.5 Thomson Reuters mantendrá un plan formal de respuesta a incidentes para responder de inmediato a las infracciones sospechadas o confirmadas de Sus Datos de acuerdo con las obligaciones regulatorias y legales.

1.6 La política de Thomson Reuters con relación a las IDs de usuario y contraseñas del personal de Thomson Reuters que accede a los sistemas de Thomson Reuters incluye, pero no está limitada a, los siguientes componentes:

(i) Cada usuario tiene un identificador de cuenta o ID de usuario único;

(ii) A cada ID de usuario o cuenta se le asigna una contraseña;

(iii) Los IDs de usuario se agregan, modifican, y eliminan de conformidad con los procesos de administración de cuentas aprobados por Thomson Reuters;

(iv) Verificación de la identificación del usuario antes de restablecer la contraseña;

(v) Las contraseñas deben ajustarse a criterios definidos que incluyen longitud, requisitos de complejidad y limitaciones de reutilización;

(vi) Los IDs de usuario, contraseñas y tokens no son compartidos ni utilizados por nadie más que el usuario al que le fueron asignados;

(vii) Contraseñas temporales o predeterminadas se configuran con valores únicos y son cambiadas después del primer uso;

(viii) El cambio de contraseña de un ID de usuario es requerido por lo menos cada noventa (90) días;

(ix) Los intentos de acceso repetidos y fallidos se bloquean durante un periodo razonable y adecuado;

(x) Las sesiones inactivas se bloquean después de un periodo comercialmente razonable; y

(xi) Los IDs de usuario se desactivan después de la salida del personal.

2. DATA SECURITY CONTROLS

2.1 Application Strategy, Design, and Acquisition.

(i) Thomson Reuters will inventory applicable applications and network components and assess their business criticality.

(ii) Thomson Reuters will review critical applications regularly to ensure compliance with industry and commercially reasonable security standards.

2.2 Anti-Virus and Anti-Malware.

(i) Thomson Reuters will implement and configure industry standard anti-virus and anti-malware software on systems holding or processing Your Data for regular signature updates.

(ii) Thomson Reuters will implement threat management capabilities designed to protect systems holding or processing Your Data.

2.3 Network Security.

(i) Thomson Reuters will configure network devices (including routers and switches) according to approved lockdown standards.

(ii) Thomson Reuters will segregate the data center networks into separate logical domains with the network security controls approved by its security personnel.

2.4 Web and Application Security.

(i) Thomson Reuters will maintain commercially reasonable security measures for internet-accessible applications, including:

(a) Implementing processes for developing secure applications;

(b) Performing pre-deployment and ongoing security assessments of internet-accessible applications;

(c) Developing internet-accessible applications based on secure coding guidelines such as those found in the Open Web Application Security Project (OWASP) Development Guide; and

(d) Validating the input, internal processing, and output of data in internet-accessible application(s).

(ii) Thomson Reuters will implement a change management process for documenting and executing operational changes in Services.

2.5 Compliance.

(i) Thomson Reuters will establish and adhere to policies that comply with laws and regulations that are applicable to Thomson Reuters and its provision of Services. Thomson Reuters does not determine whether Your Data includes information subject to any specific law or regulation and compliance with any such law or regulation is the sole responsibility of the Customer.

(ii) To the extent legally permitted, Thomson Reuters will endeavor to notify Customer promptly after Thomson Reuters receives

2. CONTROLES DE SEGURIDAD DE DATOS

2.1 Estrategia, Diseño y Adquisición de Aplicaciones.

(i) Thomson Reuters realizará un inventario de aplicaciones y componentes de red aplicables y evaluará su criticidad comercial.

(ii) Thomson Reuters revisará las aplicaciones críticas con regularidad para garantizar el cumplimiento de los estándares de seguridad comercialmente razonables y de la industria.

2.2 Antivirus y Antimalware.

(i) Thomson Reuters implementará y configurará el software antivirus y antimalware estándar de la industria en los sistemas que almacenan o procesan Sus Datos para actualizaciones periódicas de firmas.

(ii) Thomson Reuters implementará capacidades de gestión de amenazas diseñadas para proteger los sistemas que contienen o procesan Sus Datos.

2.3 Seguridad de la Red.

(i) Thomson Reuters configurará los dispositivos de red (incluidos enrutadores y conmutadores) de acuerdo con los estándares de bloqueo aprobados.

(ii) Thomson Reuters segregará las redes del centro de datos en dominios lógicos separados con los controles de seguridad de la red aprobados por su personal de seguridad.

2.4 Seguridad Web y de Aplicaciones.

(i) Thomson Reuters mantendrá medidas de seguridad comercialmente razonables para las aplicaciones accesibles por Internet, que incluyen:

(a) Implementación de procesos para el desarrollo de aplicaciones seguras.

(b) Realización de evaluaciones de seguridad previas a la implementación y continuas de aplicaciones accesibles por Internet.

(c) Desarrollar aplicaciones accesibles por Internet basadas en pautas de codificación segura, como las que se encuentran en la Guía de Desarrollo del Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP); y

(d) Validar la entrada, el procesamiento interno y la salida de datos en aplicaciones accesibles por Internet.

(ii) Thomson Reuters implementará un proceso de gestión de cambios para documentar y ejecutar cambios operativos en los Servicios.

2.5 Cumplimiento.

(i) Thomson Reuters establecerá y se adherirá a políticas que cumplan con las leyes o reglamentos que sean aplicables a Thomson Reuters y a la prestación de sus Servicios. Thomson Reuters no determina si Sus Datos incluyen información sujeta a alguna ley o reglamento específico y el cumplimiento de dicha ley o reglamento es responsabilidad exclusiva del Cliente.

(ii) En la medida legalmente permitida, Thomson Reuters se esforzará por notificar al Cliente con prontitud después de que Thomson Reuters

correspondence or a complaint from a government or regulatory official or agency related to the security of Your Data. For purposes of the foregoing, a correspondence or complaint excludes normal customer service correspondence or inquiries.

2.6 Physical and Environmental Security.

Thomson Reuters Services will be housed in secure facilities protected by a secure perimeter, with generally accepted industry standard security barriers and entry controls for providers of similar services, including:

(i) Such Thomson Reuters facilities will be physically protected from unauthorized access, damage, and interference;

(ii) Access to such facilities will be logged and logs will be maintained;

(iii) Procedures will be maintained for visitors and guests accessing such Thomson Reuters facilities; and

(iv) Thomson Reuters will employ physical safeguards designed to protect Thomson Reuters Services systems from security threats and environmental hazards.

2.7 Security Testing and Patching.

(i) Thomson Reuters will perform security testing for common security coding errors and vulnerabilities against systems holding or processing Your Data in line with generally accepted industry standards.

(ii) Thomson Reuters will regularly scan systems holding or processing Your Data for security vulnerabilities.

(iii) Thomson Reuters will follow a commercially reasonable and industry standard security patching process.

2.8 Exchange, Transfer, and Storage of Information.

(i) Thomson Reuters shall ensure that all account usernames and authentication credentials are stored and transmitted across networks and protected with a minimum of 128 AES encryption. Thomson Reuters shall not store user credentials in clear text under any circumstances. Your Data shall be encrypted at a minimum of 256 AES when in transit and at rest. Thomson Reuters will also use encryption for Your Data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws. Thomson Reuters will hold such encryption keys in the strictest of confidence and limit access to only named individuals with a need to have access.

(ii) Your Data will not be stored or transported on a laptop or any other mobile device or storage media, including USB, DVDs, or CDs, unless encrypted using a commercially reasonable encryption methodology. All electronic data transfers of Your Data by Thomson Reuters will be transmitted via SFTP or other commercially reasonable encrypted form.

2.9 Penetration Testing, Monitoring, Vulnerabilities.

(i) Thomson Reuters or an appointed third party may periodically perform penetration testing on the Thomson Reuters systems

reciba correspondencia o una queja de parte de un oficial o agencia de gobierno o regulatoria relacionada con la seguridad de Sus Datos. Para efectos de lo anterior, correspondencia o queja excluye la correspondencia o consultas normales de servicio al cliente.

2.6 Seguridad Física y Ambiental.

Los Servicios de Thomson Reuters se alojarán en instalaciones seguras protegidas por un perímetro seguro, con barreras de seguridad y controles de entrada estándar en la industria generalmente aceptados para proveedores de servicios similares, que incluyen:

(i) Dichas instalaciones de Thomson Reuters estarán protegidas físicamente contra accesos no autorizados, daños e interferencias.

(ii) El acceso a dichas instalaciones se registrará y se mantendrán registros;

(iii) Se mantendrán procedimientos para visitantes e invitados que accedan a dichas instalaciones de Thomson Reuters; y

(iv) Thomson Reuters empleará protecciones físicas diseñadas para proteger los sistemas de Servicios de Thomson Reuters de amenazas a la seguridad y peligros ambientales.

2.7 Pruebas de Seguridad y Parches.

(i) Thomson Reuters realizará pruebas de seguridad para detectar vulnerabilidades y errores de codificación de seguridad comunes contra los sistemas que almacenan o procesan Sus Datos de acuerdo con los estándares generalmente aceptados de la industria.

(ii) Thomson Reuters escaneará regularmente los sistemas que contienen o procesan Sus Datos en busca de vulnerabilidades de seguridad.

(iii) Thomson Reuters seguirá un proceso de aplicación de parches de seguridad comercialmente razonable y estándar de la industria.

2.8 Intercambio, Transferencia y Almacenamiento de Informaciones.

(i) Thomson Reuters se asegurará de que todos los nombres de usuario de las cuentas y las credenciales de autenticación sean almacenadas y transmitidas a través de las redes y que estén protegidos con un mínimo de encriptación 128 AES. Thomson Reuters no deberá almacenar credenciales de usuario en "*texto no cifrado*" en ninguna circunstancia. Sus Datos deberán ser encriptados con un mínimo de 256 AES cuando estén en tránsito y en reposo. Thomson Reuters también utilizará encriptación para que Sus Datos sean transmitidos a través de la Internet pública o de forma inalámbrica y según sea requerido por las leyes aplicables. Thomson Reuters mantendrá dichas claves de encriptación en la más estricta confidencialidad y limitará el acceso únicamente a determinadas personas que tengan la necesidad de tener acceso.

(ii) Sus Datos no serán almacenados ni transportados en una computadora portátil ni en ningún otro dispositivo móvil o medio de almacenamiento, incluidos USB, DVDs o CDs, a menos que sean encriptados utilizando un método de encriptación comercialmente razonable. Todas las transferencias electrónicas de Sus Datos realizadas por Thomson Reuters serán transmitidos mediante SFTP o cualquier otra forma de encriptación comercialmente razonable.

2.9 Pruebas de Penetración.

(i) Thomson Reuters o un tercero designado puede realizar periódicamente pruebas de penetración en los sistemas de Thomson

supporting the Services. Upon written request, Thomson Reuters shall make available to Costumer a summary on the outcome of such relevant penetration testing or an executive summary of the penetration testing results.

(ii) Thomson Reuters will monitor the relevant Thomson Reuters information systems for security threats, misconfigured systems, and vulnerabilities on an ongoing basis.

(iii) Thomson Reuters will classify any vulnerability findings identified as emergency, critical, high, medium, or low in accordance with generally accepted industry standards for providers of similar services, and in accordance with Thomson Reuters risk assessment policies. Although the actual timeframe needed to affect such remediation will depend on the nature of the finding, Thomson Reuters will undertake commercially reasonable efforts to correct vulnerabilities according to the following timeframes:

Vulnerability Classification	Definition	Remediation Goal
Emergency	A vulnerability that has a high probability of being widely exploited in a manner disruptive to normal business operations.	Begin deployment of patches and mitigations promptly, without undue delay, and complete remediation activities within seven (7) days
Critical	A vulnerability that has a high probability of being exploited that could result in broad exposure of confidential information or disruption of service, but the nature of the vulnerability does not reach the level of an "emergency" risk.	Without undue delay and in any event within thirty (30) days
High Risk	A vulnerability that has a reasonably high probability of being exercised that could allow broad exposure or compromise of confidential information or disruption of service.	Without undue delay and in any event within sixty (60) days
Medium Risk	A vulnerability that has a medium probability of being exercised.	Without undue delay and in any event within ninety (90) days
Low Risk	A vulnerability that has a low probability of being exercised.	Best efforts to address vulnerability in accordance with Thomson Reuters risk management policies. Depending on the scope of the vulnerability, correction may be addressed in the next scheduled update.

Reuters que respaldan los Servicios. Previa solicitud por escrito, Thomson Reuters pondrá a disposición del Cliente un resumen del resultado de dichas pruebas de penetración relevantes o un resumen ejecutivo de los resultados de las pruebas de penetración.

(ii) Thomson Reuters monitoreará los sistemas de información relevantes de Thomson Reuters para detectar amenazas de seguridad, sistemas mal configurados y vulnerabilidades de manera continua.

(iii) Thomson Reuters clasificará cualquier hallazgo de vulnerabilidad identificado como emergencia, crítica, alta, media o baja de acuerdo con los estándares de la industria generalmente aceptados para proveedores de servicios similares, y de acuerdo con las políticas de evaluación de riesgos de Thomson Reuters. Aunque el plazo real necesario para efectuar dicha corrección dependerá de la naturaleza del hallazgo, Thomson Reuters empleará esfuerzos comercialmente razonables para corregir las vulnerabilidades de conformidad con los siguientes plazos:

Clasificación Vulnerabilidad	Definición	Objetivo de Corrección
Emergencia	Una vulnerabilidad que tiene una alta probabilidad de ser explotada ampliamente de manera disruptiva para las operaciones comerciales normales.	Comenzar la implementación de parches y mitigaciones rápidamente, sin demoras indebidas y completar las actividades de corrección dentro de siete (7) días
Crítica	Una vulnerabilidad que tiene una alta probabilidad de ser explotada que puede resultar en una exposición amplia de información confidencial o interrupción del servicio, pero la naturaleza de la vulnerabilidad no alcanza el nivel de un riesgo de "emergencia"	Sin demoras indebidas y en cualquier caso dentro de treinta (30) días
Riesgo Alto	Una vulnerabilidad que tiene una probabilidad razonablemente alta de ocurrir y que podría permitir una amplia exposición o comprometer información confidencial o interrupción del servicio.	Sin demoras indebidas y en cualquier caso dentro de sesenta (60) días
Riesgo Medio	Una vulnerabilidad que tiene una probabilidad media de ser ocurrir.	Sin demoras indebidas y en cualquier caso dentro de noventa (90) días
Riesgo Bajo	Una vulnerabilidad que tiene una probabilidad baja de ocurrir.	Mejores esfuerzos para atender la vulnerabilidad de conformidad con las políticas de manejo de riesgos de Thomson Reuters. Dependiendo del alcance de la vulnerabilidad la corrección podrá ser atendida en la siguiente actualización

		calendarizada.

2.10 Personnel Access. Thomson Reuters will implement controls designed to manage personnel´s access to systems supporting the Services to be granted on a need-to-know basis consistent with assigned job responsibilities, which may include the use of role-based access controls to help ensure appropriate access rights, permissions, and segregation of duties.

2.10 Acceso del Personal. Thomson Reuters implementará controles diseñados para gestionar el acceso de su personal a los sistemas que respaldan los Servicios, mismo que se otorgará con base la necesidad de conocer de acuerdo con las responsabilidades laborales asignadas, que podrán incluir el uso de controles de acceso basados en su rol para ayudar a garantizar derechos de acceso, permisos y segregación de funciones adecuadas.

2.11 Segregation of Data. Thomson Reuters agrees that Your Data hosted within the Services in a production environment is maintained so as to preserve logical segregation of Your Data from data of others.

2.11 Segregación de Datos. Thomson Reuters acepta que Sus Datos alojados dentro de los Servicios en un entorno de producción se mantienen así para preservar una segregación lógica de Sus Datos de los datos de otros.

2.12 Data Removal, Deletion and Destruction. If not otherwise set forth in the applicable Agreement, upon conclusion or termination of the Services at the written request of the Customer, Thomson Reuters will securely destroy and, upon request, confirm the destruction of all copies of Your Data in any electronic or non-electronic form, except (i) for backup or archival copies kept in the normal course of business, including as part of a defined data retention program; or (ii) to the extent necessary to comply with applicable law and regulations.

2.12 Eliminación y Destrucción de Datos. Si no se establece lo contrario en el Contrato correspondiente, al concluir o cancelar los Servicios a pedido por escrito del Cliente, Thomson Reuters destruirá de forma segura y, previa solicitud, confirmará la destrucción de todas las copias de Sus datos en cualquier forma electrónica o no electrónica excepto (i) para copias de seguridad o de archivo mantenidas en el curso normal del negocio, incluso como parte de un programa definido de retención de datos; o (ii) en la medida necesaria para cumplir con las leyes y regulaciones aplicables.

2.13 Adjustment of Data Security Controls. Thomson Reuters will evaluate and may adjust its data security controls in light of: (i) the results of the testing monitoring; (ii) any material changes to Thomson Reuters operations or business arrangements; (iii) the results of risks assessments performed; or (iv) any other circumstances that Thomson Reuters knows or has reason to know may have a material impact on its data security controls.

2.13 Ajuste a los Controles de Seguridad de Datos. Thomson Reuters evaluará y podrá ajustar sus controles de seguridad de datos a la luz de: (i) los resultados del monitoreo de pruebas; (ii) cualesquier cambios materiales a las operaciones o acuerdos comerciales de Thomson Reuters; (iii) los resultados de las evaluaciones de riesgo realizadas; o (iv) cualesquier otras circunstancias que Thomson Reuters conozca o tenga motivos para conocer que pudieran tener un impacto material en sus controles de seguridad de datos.

3. SECURITY QUESTIONNAIRES AND ASSESSMENTS

3.1 No more than once per calendar year, Customer may request Thomson Reuters in writing to complete an information security questionnaire, or by way of a secure portal, be provided with a pre-populated security questionnaire in an industry recognized format. Thomson Reuters agrees to respond to such questionnaire as soon as commercially reasonable. Customers who purchase multiple products under one or more agreements will coordinate requests into a single questionnaire per calendar year. You agree that the information contained in such responses are the proprietary and confidential information of Thomson Reuters.

3.2 To the extent Thomson Reuters performs and makes available to customers an independent third-party assessment or certification with respect to that service (e.g. ISO 27001, SOC 2), upon Customer's request, Customer may review an available executive summary of the results of such security assessments for the Services containing Your Data. You agree that the information contained in such assessments, certification, or executive summary are the proprietary and confidential information of Thomson Reuters.

3. CUESTIONARIOS Y EVALUACIONES DE SEGURIDAD

3.1 No más de una vez por año calendario, el Cliente puede solicitar a Thomson Reuters por escrito que complete un cuestionario de seguridad de la información o, a través de un portal seguro, que se le proporcione un cuestionario de seguridad rellenado previamente en un formato reconocido por la industria. Thomson Reuters acepta responder a dicho cuestionario tan pronto como sea comercialmente razonable. Los Clientes que compren múltiples productos bajo uno o más acuerdos coordinarán las solicitudes en un solo cuestionario por año calendario. Usted acepta que la información contenida en dichas respuestas es información confidencial y propiedad de Thomson Reuters.

3.2 En la medida en que Thomson Reuters realice y ponga a disposición de los clientes una evaluación o certificación de un tercero independiente con respecto a ese servicio (por ejemplo, ISO 27001, SOC 2), a pedido del Cliente, el Cliente puede revisar un resumen ejecutivo disponible de los resultados de dichas evaluaciones de seguridad para los Servicios que contienen Sus Datos. Usted acepta que la información contenida en dichas evaluaciones, certificaciones o resúmenes ejecutivos es información confidencial y propiedad de Thomson Reuters

4. NOTIFICATION OF SECURITY BREACH

4.1 Thomson Reuters will, without undue delay but in any event within seventy-two (72) hours of discovery, notify Customer of a Security Breach. Thomson Reuters agrees that it will not inform any third party of any Security Breach naming you without first obtaining Customers´ prior written consent, unless if (i) required by applicable law or regulation; or (ii) such disclosure is in the furtherance of a

4. NOTIFICACIÓN DE VIOLACIÓN DE SEGURIDAD

4.1 Thomson Reuters notificará, sin demora indebida, pero en cualquier caso dentro de las setenta y dos (72) horas del descubrimiento, al Cliente sobre una Violación de la Seguridad. Thomson Reuters acepta que no informará a ningún tercero sobre ninguna Violación de Seguridad que lo nombre a usted sin primero obtener previo consentimiento por escrito del Cliente, a menos que (i) sea requerido

Thomson Reuters security breach investigation or the execution of its response plan.

4.2 In the event of any such Security Breach, Thomson Reuters will take commercially reasonable measures and actions to remedy or mitigate the effects of the Security Breach and will perform a root cause analysis to identify the cause of such Security Breach.

4.3 Upon Customer's reasonable request, Thomson Reuters may provide documentation related to such Security Breach, including, to the extent known, a summary of the cause of such Security Breach and steps taken to remedy the Security Breach and to prevent a reoccurrence. Thomson Reuters will reasonably cooperate with Customer in seeking injunctive or other equitable relief against any third party deemed responsible or complicit in the Security Breach.

4.4 If legally permitted, in the event of a Security Breach, Thomson Reuters agrees to reasonably cooperate with Customer with protecting its rights relating to the use, disclosure, protection, and maintenance of Your Data.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

Thomson Reuters will, at all times while this Agreement is in effect, maintain a Business Continuity and Disaster Recovery Plan. Thomson Reuters will perform periodic testing of its Business Continuity and Disaster Recovery Plan to confirm its effectiveness. Upon Customer request, Thomson Reuters will provide a high-level report about the outcome of its latest Business Continuity and Disaster Recovery Plan test.

6. SERVICES RESILIENCE

6.1 Thomson Reuters will use commercially reasonable efforts to restore the Services by having offline backups of application data, infrastructure components and configuration settings.

6.2 Thomson Reuters will use commercially reasonable efforts to protect Services that host or process Your Data against denial- of-service attacks by implementing denial-of-service mitigation solutions.

7. SHARED SECURITY OBLIGATIONS

You agree that you are responsible for all transactions that occur on your account and that it is your responsibility to ensure that you and your users use unique usernames and strong passwords for each account used to access the Services. You agree that you and your users must hold in confidence all usernames and passwords used for accessing the Services, and each user must immediately change their username/password combinations that have been acquired by or disclosed to an unauthorized third party. You also agree to enroll and require your personnel and other users to enroll in multi-factor authentication ("MFA") where made available to you, and you are responsible for all transactions and other activity that would have been prevented by the proper use of MFA. Additionally, you will notify Thomson Reuters if you become aware of any unauthorized third-party access to Thomson Reuters data or systems and will use reasonable efforts to remedy identified security threats and vulnerabilities to your systems.

por la ley o reglamento aplicable; o (ii) dicha divulgación es para promover una investigación de una violación de seguridad de Thomson Reuters o en la ejecución de su plan de respuesta.

4.2 En el caso de dicha Violación de la Seguridad, Thomson Reuters tomará medidas y acciones comercialmente razonables para remediar o mitigar los efectos de la Violación de la Seguridad y realizará un análisis de causa raíz para identificar la causa de dicha Violación de la Seguridad.

4.3 A pedido razonable del Cliente, Thomson Reuters puede proporcionar documentación relacionada con dicha Violación de la Seguridad, incluido, en la medida en que se conozca, un resumen de la causa de dicha Violación de la Seguridad y los pasos tomados para remediar la Violación de la Seguridad y evitar que vuelva a ocurrir. Thomson Reuters cooperará razonablemente con el Cliente en la búsqueda de medidas cautelares u otras medidas equitativas contra cualquier tercero que se considere responsable o cómplice de la Violación de la Seguridad.

4.4 Si estuviera legalmente permitido, en caso de una Violación de Seguridad, Thomson Reuters acepta cooperar razonablemente con el Cliente para proteger sus derechos relacionados con el uso, divulgación, protección, y mantenimiento de Sus Datos.

5. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES

Thomson Reuters, en todo momento mientras este Acuerdo esté vigente, mantendrá un Plan de Continuidad Comercial y Recuperación de Desastres. Thomson Reuters realizará pruebas periódicas de su Plan de Continuidad Comercial y Recuperación de Desastres para confirmar su eficacia. A solicitud del Cliente, Thomson Reuters proporcionará un reporte de alto nivel sobre los resultados de su última prueba del Plan de Continuidad Comercial y Recuperación de Desastres.

6. RESILIENCIA DE SERVICIOS

6.1 Thomson Reuters hará todos los esfuerzos comercialmente razonables para restaurar los Servicios mediante copias de seguridad fuera de línea de los datos de la aplicación, los componentes de la infraestructura y los ajustes de configuración.

6.2 Thomson Reuters hará todos los esfuerzos comercialmente razonables para proteger los Servicios que alojan o procesan Sus Datos contra ataques de denegación de servicio mediante la implementación de soluciones de mitigación de denegación de servicio.

7. OBLIGACIONES DE SEGURIDAD COMPARTIDAS

Usted acepta que usted es responsable por todas las transacciones que ocurran en su cuenta y que es su responsabilidad asegurar que usted y sus usuarios usen nombres de usuario únicos y contraseñas seguras para cada cuenta usada para acceder a los Servicios. Usted acepta que usted y sus usuarios deben mantener confidenciales todos los nombres de usuario y contraseñas utilizados para acceder a los Servicios, y cada usuario debe cambiar de inmediato sus combinaciones de nombre de usuario/contraseña que hayan sido adquiridas o divulgadas a un tercero no autorizado. Usted también acepta inscribirse y requerir a su personal y otros usuarios se inscriban al método de autenticación multi factor ("AMF") cuando esté disponible para usted, y usted es responsable de todas las transacciones y otras actividades que pudieran haber sido evitadas mediante el uso adecuado de la AMF. Además, usted notificará a Thomson Reuters si tiene conocimiento de cualquier acceso no autorizado de terceros a los datos o sistemas de Thomson Reuters y hará todos los esfuerzos razonables para remediar las amenazas de seguridad y vulnerabilidades identificadas en sus

8. BACKGROUND CHECKS

Employment background checks serve as an important part of Thomson Reuters selection process. Verifying background information validates a candidate's overall employability or an employee's suitability for a particular assignment. Depending on the country and position at issue, to the extent as is customary and permitted by law, all Thomson Reuters background checks may include identification verification, prior employment verification, criminal background information, global terror/sanctions checks and education verification. Thomson Reuters agrees to use qualified information security personnel to perform data security services.

9. DEFINITIONS

(i) **"Agreement"** means the underlying agreement between Thomson Reuters and Customer for the provision of Services that references and incorporates this Addendum.

(ii) **"Business Continuity and Disaster Recovery Plan"** means a business continuity, contingency and disaster recovery activation plan to minimize disruption in and reinstate the operation of the use of the Services by you due to a disaster or similar event.

(iii) **"Documentation"** means manuals, handbooks, guides and other instructions, documentation and materials available through the product or provided by us regarding the capabilities, operation, and use of our Services.

(iv) **"Professional Services"** means the implementation, customization, training, consulting or other professional services we provide, as may be described in the applicable Agreement.

(v) **"Property"** means our property, which includes, but is not limited to, our products, Services, information, Documentation, data (whether tangible or intangible) and Usage Information.

(vi) **"Security Breach"** means a confirmed breach of security that results in the unauthorized destruction, loss, alteration, disclosure of, or access to Your Data where such breach of security is likely to result in a significant risk of harm to you or your Data Subject(s) or where Thomson Reuters is required by applicable data protection law to notify you thereof.

(vii) **"Services"** means the cloud computing services, software-as- a-service, online research services, Professional Services, as well as any products, including installed software, supplied by Thomson Reuters that are detailed in the applicable Agreement.

(viii) **"Usage Information"** means any information, data, or other content (including statistical compilations and performance information) related to or derived from your access to and use of our Property.

(ix) **"Your Data**" means information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by you or on your behalf through the Services. For clarity, Your Data does not include any information belonging to Thomson Reuters or its licensors, including without limitation: any content provided by

sistemas.

8. VERIFICACIONES DE ANTECEDENTES

Las verificaciones de antecedentes laborales son una parte importante del proceso de selección de Thomson Reuters. La verificación de la información de antecedentes valida la empleabilidad general de un candidato o la idoneidad de un empleado para una tarea en particular. Según el país y el cargo en cuestión, en la medida en que sea habitual y lo permita la ley, todas las verificaciones de antecedentes de Thomson Reuters pueden incluir verificación de identificación, verificación de empleo previo, información de antecedentes penales, verificación de sanciones/terrorismo y verificación de educación. Thomson Reuters acepta emplear personal de seguridad de la información calificado para llevar a cabo los servicios de seguridad de datos.

9. DEFINICIONES

(i) **"Contrato"** significa el contrato celebrado entre Thomson Reuters y el Cliente para la prestación de Servicios que hace referencia e incorpora esta Adenda.

(ii) **"Plan de Continuidad Comercial y Recuperación de Desastres"** significa un plan de activación de continuidad comercial, contingencia y recuperación ante desastres para minimizar la interrupción y restablecer la operación del uso de los Servicios debido a un desastre o evento similar

(iii) **"Documentación"** significa manuales, instructivo, guías y otras instrucciones, documentación y materiales disponibles a través del producto o proporcionados por nosotros relacionados con las capacidades, operación y uso de nuestros Servicios.

(iv) **"Servicios Profesionales"** se refiere a la implementación, personalización, capacitación, consultoría u otros servicios profesionales que brindamos, tal como se describe en el Contrato correspondiente.

(v) **"Propiedad"** significa nuestra propiedad, que incluye, pero no se limita a, nuestros productos, Servicios, información, Documentación, datos (ya sea tangibles o intangibles) e Información de Uso.

(vi) **"Violación de la Seguridad"** significa una violación confirmada de la seguridad que resulta en la destrucción, pérdida, alteración, divulgación o acceso no autorizados a Sus Datos donde es probable que dicha violación de la seguridad resulte en un riesgo significativo de daño para usted o al Titular de los Datos(s) en su posesión o cuando la ley de protección de datos aplicable requiera que Thomson Reuters se lo notifique.

(vii) **"Servicios"** se refiere a los servicios de computación en la nube, software como servicio, servicios de investigación en línea, Servicios Profesionales, así como cualquier producto, incluido el software instalado, suministrado por Thomson Reuters que se detalla en el Contrato correspondiente.

(viii) **"Información de Uso"** se refiere a cualquier información, datos o cualquier contenido (incluidas las compilaciones estadísticas y la información de rendimiento) relacionada con o derivada de su acceso y uso de nuestra Propiedad.

(ix) "**Sus Datos**" significa información, datos y otro contenido, en cualquier forma o medio, que usted o en su nombre envía, pública o transmite de otra manera a través de los Servicios. Para mayor claridad, Sus Datos no incluyen ninguna información que pertenezca a Thomson Reuters o sus licenciantes, incluidos, entre otros: cualquier

Thomson Reuters as part of the Services, authentication and security information, billing and customer relationship information, marketing information, and Usage Information.

contenido proporcionado por Thomson Reuters como parte de los Servicios, información de autenticación y seguridad, información de facturación y relación con el cliente, información de marketing e Información de Uso.

The Parties agree that in case of controversy between the English and Spanish versions of these terms, the English version will prevail.

Las Partes acuerdan que, en caso de controversia entre las versiones en inglés y español de estos términos, prevalecerá la versión en inglés.