Thomson Reuters Data Security Addendum

Version 2.0

Last Modified: November 3, 2023

Adenda de Seguridad de Datos de Thomson Reuters

Versión 2.0

Última Modificación: 03 de noviembre de 2023

This Data Security

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

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)

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.

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 *texto no cifrado* 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

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

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.

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 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.

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

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.