Experian Supplier Security Requirements (Summary)

The security requirements included in this document are intended to provide the potential supplier a summary of the key control areas which are expected to form the basis of the supplier's "Information Security Program". This programme shall be in effect to protect Experian Information the supplier receives, processes, transfers, transmits, stores, delivers, and / or otherwise accesses.

DEFINITIONS

"Experian Information" means Experian data files, databases, applications software (source code and object code), software documentation, supporting process documents, operational process and procedure documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, business information, and other data specifically classified by Experian as confidential or restricted.

"Resource" means all Supplier devices, including but not limited to laptops, PCs, routers, servers, and other computer systems that store, process, transfer, transmit, deliver or otherwise access the Experian Information.

INFORMATION SECURITY PROGRAM

Supplier will maintain a comprehensive Information Security Program that contains administrative, technical, and physical safeguards appropriate to the complexity, nature, and scope of its activities, and the sensitivity of its information assets. Such safeguards will include the elements set forth below and will be reasonably designed to:

(1) achieve the security and confidentiality of Experian Information;

(2) protect against any anticipated threats or hazards to the security or integrity of Experian Information;

(3) protect against unauthorised access to or use of Experian Information that could result in substantial harm or inconvenience to Experian, its clients and / or consumers, and

(4) provide assurances to Experian of the ongoing effectiveness of controls.

Requisitos de seguridad del proveedor de Experian (resumen)

Los requisitos de seguridad incluidos en este documento están destinados a proporcionar al proveedor potencial un resumen de las áreas de control clave que se espera formen la base del "Programa de seguridad de la información" del proveedor. Este programa estará vigente para proteger la información de Experian que el proveedor reciba, procese, transfiera, transmita, almacene, entregue y / o tenga acceso de otra manera.

DEFINICIONES

"Información de Experian" significa archivos de datos, bases de datos, software de aplicaciones (código fuente y código objeto), documentación de software, documentos de proceso de soporte, documentación de procesos y procedimientos operativos, planes de prueba, casos de prueba, escenarios de prueba, informes de incidentes cibernéticos, información del consumidor, información de negocio y otros datos clasificados específicamente por Experian como confidenciales o restringidos.

"Recurso" significa todos los dispositivos del Proveedor, incluidos, entre otros, equipos portátiles, PC, enrutadores, servidores y otros sistemas informáticos que almacenan, procesan, transfieren, transmiten, entregan o acceden a la Información de Experian.

PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

El Proveedor mantendrá un Programa de seguridad de la información completo que contenga controles administrativos, técnicos y físicos acordes con la complejidad, naturaleza, alcance de sus actividades y la sensibilidad de sus activos de información. Dichas salvaguardas incluirán los elementos establecidos a continuación y estarán razonablemente diseñadas para:

(1) Preservar la seguridad y confidencialidad de la información de Experian;
(2) proteger de manera anticipada contra amenazas o riesgos la seguridad o integridad de la Información de Experian;

(3) Proteger contra el acceso o uso no autorizado de la Información de Experian, que pueda llegar causar daños o perjunicioS a Experian, sus clientes y / o consumidores, y

(4) Garantizar a Experian la efectividad de los controles.

If Supplier receives, stores, processes, or transmits cardholder data (CHD; specifically, the primary account number) or sensitive authentication data (SAD)*, it must comply with the most current Payment Card Industry Data Security Standard (PCI DSS) as it relates to the processing of such data as a service provider to Experian. *For further definition see PCI Data Security Standard as published on https://www.pcisecuritystandards.org/	Si el Proveedor recibe, almacena, procesa o transmite datos del titular de la tarjeta (CHD- cardholder data), específicamente el número completo de la tarjeta o "datos sensibles de autenticación" (SAD - sensitive authentication data) *, debe cumplir con el estándar actual de seguridad de datos de la industria de tarjetas de pago "Payment Card Industry Data Security Standard" (PCI DSS) en lo que se refiere al procesamiento de datos como un proveedor de servicios de Experian. * Para una definición más detallada, consulte el Estándar de seguridad de datos PCI, publicado en https://www.pcisecuritystandards.org/
SECURITY REQUIREMENTS	**REQUERIMIENTOS DE SEGURIDAD**
1. Information Security Policies and Governance Supplier's Information Security Program will be consistent with the practices described in an industry standard such as ISO 27002 and the Experian Supplier Security Requirements Document that is aligned to the Experian Information Security policy.	**1. Políticas de gobierno y seguridad de la información** El programa de seguridad de la información del proveedor será coherente con las prácticas descritas en un estándar de la industria como ISO 27002 y el documento de requerimientos de seguridad para Proveedores de Experian, el cual está alineado con la política de seguridad de la información de Experian.
2. Confidentiality and Integrity Supplier will utilise a managed approach to security to ensure that Experian Information is protected through the entire life cycle, from creation, transformation and use, storage and destruction regardless of the storage media e.g. tape, disk, paper, etc.	**2. Confidencialidad e integridad** El proveedor utilizará un enfoque administrado de la seguridad para garantizar que la información de Experian esté protegida durante todo el ciclo de vida la misma, desde la creación, transformación, uso, almacenamiento hasta su destrucción, independientemente de los medios de almacenamiento ej: cinta, disco, papel, etc.
3. Information Stewardship Supplier will designate information stewards who are responsible for information assets under their control which store, process or transmit Experian Information.	**3. Administración de la información** El proveedor designará administradores de la información que sean responsables de los activos de información bajo su control, los cuales almacenan, procesan o transmiten la información de Experian.
4. Data Loss Protection Data Loss Prevention (DLP) solutions are to be utilised to identify, monitor and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through content inspection and with a centralised management framework.	**4. Protección de pérdida de datos** Las soluciones de prevención de pérdida de datos (Data Loss Prevention - DLP) deben utilizarse para identificar, monitorear y proteger a través de la inspección de contenido centralizada, los datos en uso, (por ej acciones en la terminal), datos en movimiento (por ej, acciones en la red) y datos en reposo (por ej, almacenamiento de datos).
5. Vulnerability Management Firewalls, routers, servers, PCs, and all other Resource(s) utilised in the provision of services to Experian will be kept current with appropriate security specific system patches. Supplier will perform regular penetration tests (including automatic and manual methods) to be completed by independent third parties to further assess the Resources.	**5. Gestión de vulnerabilidades** Los Firewalls, enrutadores, servidores, PC y todos los demás recursos utilizados en la prestación de servicios a Experian se mantendrán actualizados con los parches de de seguridad liberados por el fabricante. El proveedor realizará pruebas de penetración periódicas (incluyendo métodos automáticos y manuales) a través de terceros independientes, con el propósito de evaluar más a fondo los recursos.

6. Physical Security A security function will exist to grant, adjust, and revoke physical access to facilities where Experian Information resides or can be accessed. All Supplier sites and access to information will reside within the contractually agreed location unless otherwise approved in writing by Experian.	**6. Seguridad física** Una función de seguridad existirá para otorgar, ajustar y revocar el acceso físico a las instalaciones donde reside o se puede acceder a la información de Experian. Todos los sitios de los proveedores y el acceso a la información residirán en la ubicación acordada contractualmente, a menos que Experian apruebe lo contrario por escrito.
7. Change Management Modifications and improvements to Resource(s) must be managed through a controlled change management process. A designated 'owner' should be identified for all change requests and changes should be approved by a Change Management Group.	**7. Gestión del cambio** Las modificaciones y mejoras de los recursos deben administrarse a través de un proceso controlado de gestión de cambios. Se debe identificar un "propietario" designado para todas las solicitudes de cambio y los cambios deben ser aprobados por un Grupo de gestión de cambios.
8. Logging and Monitoring Logging mechanisms must be in place for all systems that process, transmit, or store Experian information. Logging is needed to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted or locked) and processes in place to review periodically to detect intrusions, unauthorised access, unintended activities, malicious software, or attempts of these or other actions that could compromise the security of systems processing Experian data. They will be retained for a minimum of 90 days.	**8. Registro y monitoreo** Se debe contar con mecanismos de registro para todos los sistemas que procesan, transmiten o almacenan información de Experian. El registro es necesario para identificar incidentes de seguridad, establecer responsabilidad individual y reconstruir eventos. Los registros de auditoría se conservarán en un estado protegido (es decir, cifrado o bloqueado) y se implementarán procesos para revisar periódicamente las intrusiones, el acceso no autorizado, las actividades no intencionadas, el software malicioso o los intentos de estas u otras acciones que puedan comprometer la seguridad de los sistemas. procesando datos de Experian. Los registros se conservarán durante un mínimo de 90 días.
9. Intrusion Prevention Systems Supplier will use security measures (including IPS and IDS) to protect the Supplier telecommunications system(s) and any computer system or network device that Supplier uses to provide services to Experian to reduce the risk of infiltration, hacking, access penetration by or exposure to a third-party.	**9. Sistemas de prevención de intrusiones** El Proveedor utilizará medidas de seguridad (incluidos IPS e IDS) para proteger el (los) sistema (s) de telecomunicaciones del Proveedor y cualquier sistema informático o dispositivo de red que el Proveedor utilice para proporcionar servicios a Experian para reducir el riesgo de que ocurran filtraciones, hacking, accesos no autorizado o exposición a un tercero.
10. Incident Response Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents to limit further damage to information assets and to permit identification and prosecution of violators. Supplier will report actual or suspected security violations or incidents that impact Experian to Experian within twenty-four (24) hours of Supplier's knowledge of such violation or incident.	**10. Respuesta a incidentes** Se establecerán procesos y procedimientos para responder a violaciones de seguridad y eventos e incidentes inusuales o sospechosos para limitar el daño a los activos de información y para permitir la identificación y enjuiciamiento de los infractores. El Proveedor informará las violaciones o incidentes de seguridad reales o sospechosos que afecten a Experian dentro de las veinticuatro (24) horas posteriores a la identificación de la violación o el incidente.
11. Malware Defense Supplier will use computer malware detection / scanning services and procedures.	**11. Defensa contra software malicioso** El proveedor utilizará procedimientos y servicios de detección / escaneo de malware informático.

12. Segregation of Duties and Envionments Supplier maintains controls designed to provide adequate segregation of duties among Supplier personnel, including access to systems and networks. Duties are assigned in such a manner that a person will not have conflicting duties that may result in accidental or deliberate compromise of information, systems or processes nor have the opportunity to conceal their errors or irregularities.	**12. Segregación de funciones y ambientes** El proveedor mantiene controles diseñados para proporcionar una segregación de tareas adecuada que involucre el personal del Proveedor y el acceso a sistemas y redes. Las funciones se asignan de tal manera que una persona no tenga conflictos de interes que puedan resultar en un compromiso accidental o deliberado de información, sistemas o procesos, ni tenga la oportunidad de ocultar sus errores o irregularidades.
13. Encryption and PKI All Experian Information will be encrypted in line with FIPS 140 requirements when in storage (at rest), unless Experian approved compensating controls are implemented. Laptop computers will not store Experian Information unless Experian agrees there is a business need for such storage, and if agreement is reached, Experian Information on laptops will be encrypted*.*	**13. Cifrado y PKI** Toda la información de Experian se cifrará de acuerdo con los requisitos de FIPS 140 cuando se almacena (en reposo), a menos que se implementen controles compensatorios aprobados por Experian. Los portátiles no almacenarán la información de Experian a menos que Experian acepte que existe una necesidad comercial para dicho almacenamiento, y si se llegase a un acuerdo, la información de Experian se cifrara en los portátiles.
14. Network Security Supplier will provide the following data communication security services: a) safeguard the confidentiality and integrity of all data being transmitted over any form of data network; and b) implement and maintain strong current industry best practise standard encryption techniques for all cases in which data identified as Experian Information is transmitted over any public data network. A minimum of 128-bit key encryption is required.	**14. Seguridad de la red** El proveedor proporcionará los siguientes servicios de seguridad en la comunicación de datos: a) salvaguardar la confidencialidad e integridad de todos los datos que se transmiten a través de la red de datos; y b) implementar y mantener técnicas de cifrado estándar de acuerdo con las mejores prácticas de la industria para todos los casos en los que se transmite información a través de cualquier red pública de datos. Se requiere un cifrado mínimo de 128 bits.
15. Identification, Authentication and Authorisation Each user of any Resource will have a uniquely assigned user ID to enable individual authentication and accountability. Resources will authenticate each user prior to granting every authorised access. The level of authentication required for access to any Resource is proportionate to the sensitivity of the data housed on the Resource. Access to privileged accounts will be restricted to only those people who administer the Resource; individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.	**15. Identificación, Autenticación y Autorización** Cada usuario de cualquier recurso tendrá una identificación de usuario asignada de forma exclusiva para permitir la autenticación y responsabilidad individual. Los recursos autenticarán a cada usuario antes de otorgarle acceso autorizado. El nivel de autenticación requerido para acceder a cualquier recurso es proporcional a la sensibilidad de los datos alojados en el recurso. El acceso a cuentas privilegiadas estará restringido solo a aquellas personas que administren el Recurso; la responsabilidad individual se mantendrá. Todas las contraseñas predeterminadas (como las de los proveedores de hardware o software) se cambiarán inmediatamente después de su recepción.
16. User Passwords and Accounts User passwords will: a) remain confidential and will not be shared, posted, or otherwise divulged in any manner; b) consist of a minimum of eight (8) characters for standard user accounts (ten character for privileged user accounts);	**16. Contraseñas y cuentas de usuario** Las contraseñas de los usuarios cumplirán con los siguientes requerimientos: a) Permanecer confidenciales y no compartir, publicar ni divulgar de ninguna manera; b) Tener una longitud mínima de ocho (8) caracteres para cuentas de usuario estándar (diez caracteres para cuentas de usuario con privilegios);

c) contain at least three of the following i. uppercase characters (A through S) ii. lowercase characters (a through s) iii. numeric characters (0 through 9) iv. non-alphabetic characters (for example, !, $, #, %) d) not contain the account name or account ID or other easily guessed values; e) not allow the previous thirteen passwords to be reused; and f) be encrypted in storage and transmission User accounts will: a) automatically lockout after five (5) consecutive incorrect attempts; and b) expire after a maximum of 90 calendar days (30 days if privileged account user)	c) Estar compuestas al menos por tres de los siguientes requerimientos i. Caracteres en mayúscula (A a S) ii. Caracteres en minúscula (a través de s) iii. Caracteres numéricos (0 a 9) iv. Caracteres especiales (por ejemplo,!, $, #,%) d) No contener el nombre de la cuenta o la identificación de la cuenta u otros valores fáciles de adivinar; e) No permitir que las trece contraseñas anteriores sean reutilizadas; y f) Cifrar tanto en el almacenamiento como la transmisión Las cuentas de usuario: a) bloqueo automático después de cinco (5) intentos incorrectos consecutivos; y b) vencer después de un máximo de 90 días calendario (30 días si el usuario de la cuenta privilegiada)
17. Remote Access Connection Authorisation All remote access connections to Supplier internal networks and / or computer systems will require authorisation and will provide an approved means of access control at the “point of entry” to the Supplier computing or communication resources through multi-factor authentication. Such access will use secure access channels, such as a Virtual Private Network (VPN).	**17. Autorización de conexión de acceso remoto** Todas las conexiones de acceso remoto a las redes internas y / o sistemas informáticos de los proveedores requerirán autorización y proporcionarán un medio de control de acceso aprobado en el "punto de entrada" a los recursos informáticos o de comunicación del proveedor a través de multiple factor de autenticación. Dicho acceso utilizará canales de acceso seguros, como una red privada virtual (VPN).
18. Secure System Development Applications developed by Supplier for Experian will follow a methodology that allows for: (i) defining security requirements as part of the requirements definition phase; (ii) using a design model that incorporates best practices in security; (iii) developing code in ways that minimise security vulnerabilities (such as cross-site scripting, SQL injection, buffer overflows, etc.); (iv) testing the code through static and dynamic assessments; and (v) deploying the application in a secure production environment.	**18. Desarrollo de sistema seguro** Las aplicaciones desarrolladas por el Proveedor para Experian seguirán una metodología que permite: (i) definir los requisitos de seguridad como parte de la fase de definición de requerimientos; (ii) usar un modelo de diseño que incorpore las mejores prácticas en seguridad; (iii) desarrollar código de forma que minimice las vulnerabilidades de seguridad (como cross-site scripting, SQL injection, buffer overflows, etc.); (iv) probar el código a través de pruebas estáticas y dinámicas; y (v) implementar la aplicación en un entorno de producción seguro.
19. Personnel Security All Supplier personnel and subcontractors, if any, who will: (a) have access to an Experian network; (b) have access to, or the capability to view or use Experian information; or (c) be on Experian premises for more than one day and issued an access badge (Individuals who are issued visitor badges and are escorted onsite by an Experian staff member for the entirety of their visit do not fall under this criterion) must pass a criminal background check, and general background investigation. Supplier shall not be required to screen any individual where it is prohibited by law.	**19. Seguridad del personal** Todo el personal y subcontratistas del Proveedor, si los hubiere, que: (a) tengan acceso a una red de Experian; (b) tengan acceso o la capacidad de ver o usar la información de Experian; o (c) se encuentren en las instalaciones de Experian por más de un día y que se les ha entregado un distintivo de acceso (las personas a las que se expiden distintivos de visitante y que son acompañadas en el sitio por un miembro del personal de Experian durante la totalidad de su visita no entran dentro de este criterio) deben aprobar un verificación de antecedentes penales e investigación general de antecedentes. El proveedor no tendrá que validar a ningún individuo donde la ley lo prohiba.

20. Training and Awareness Supplier shall require all Supplier personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel. Where Supplier has direct access to Experian systems and / or network, Supplier personnel may be mandated to complete Experian training and awareness programs.	**20. Entrenamiento y Conciencia** El proveedor deberá exigir a todo su personal que participe en las sesiones de capacitación y concientización sobre seguridad de la información al menos una vez al año y que establezca pruebas de aprendizaje para todo el personal. Cuando el Proveedor tenga acceso directo a los sistemas y / o la red de Experian, es mandatorio que el personal del Proveedor complete los programas de capacitación y concientización de Experian.
21. Business Continuity Supplier will implement and maintain a Business Continuity program that includes documented recovery strategies, plans and procedures, to ensure the Supplier can continue to deliver its products and services to Experian within the contractual recovery time objective.	**21. Continuidad del negocio** El Proveedor implementará y mantendrá un programa de Continuidad del Negocio que incluye estrategias, planes y procedimientos de recuperación documentados para garantizar que el Proveedor pueda continuar entregando sus productos y servicios a Experian dentro del tiempo objetivo de recuperación contractual.
22. Experian's Right to Audit Experian may conduct audits and onsite security risk assessments to assess Supplier Information Security Program and Supplier's compliance with Experian Supplier Security Requirements.	**22. El derecho de Experian a la auditoría** Experian puede realizar auditorías y evaluaciones de riesgos de seguridad en el sitio para evaluar el Programa de seguridad de la información del proveedor y el cumplimiento del proveedor con los requisitos de seguridad del proveedor de Experian.
23. Third Party Relationships Supplier will not provide or commence work with any third party that impacts Experian Information without the prior written approval of Experian. Supplier will not use offshore resources without the prior written approval of Experian. Supplier will conduct security risk assessments of any third-party service providers with access to Experian Information.	**23. Relaciones con terceros** El Proveedor no trabajará con ningún tercero que afecte la Información de Experian sin la aprobación previa de Experian por escrito. El proveedor no utilizará recursos externos sin la aprobación previa por escrito de Experian. El proveedor llevará a cabo evaluaciones de riesgos de seguridad de cualquier tercero proveedor de servicios con acceso a la información de Experian.