Proveedor: Denominación / Nombre y apellidos:	
NIF:	

Clausulado de Seguridad de la Información

El Proveedor se compromete y obliga al cumplimiento de todas las normas de seguridad desarrolladas por Aliseda, que se describen en este Anexo y que forman parte integrante de la Política de Seguridad de la Información (en adelante, la Política) a todos los efectos.

Las normas de seguridad básicas que se presentan son aplicables a todo Proveedor de Aliseda, que durante la prestación de servicios acceda, procese, transmita o almacene información de Aliseda.

Políticas de Seguridad y Propiedad de la Información

- El Proveedor debe garantizar la confidencialidad, integridad y disponibilidad de la información gestionada para Aliseda (ya sea recibida, procesada, transferida, transmitida, almacenada, entregada y/o accedida) en el ámbito del servicio, proyecto, trabajo, contrato o acuerdo prestado.
- Toda la información proporcionada, facilitada, en posesión o accesible al Proveedor en el ámbito del servicio es propiedad de Aliseda o de sus Clientes o de terceros con ellos relacionados. El Proveedor está obligado a compartir la información relativa a la Seguridad de la Información cuando Aliseda lo solicite, en todo lo relativo a usuarios, y sistemas, cambios efectuados, registro de eventos, alertas de seguridad, etc.
- El Proveedor se compromete a dar a conocer las políticas aplicables al servicio a sus empleados para asegurar su cumplimiento, detallando la normativa aplicable y las consecuencias en caso de incumplimiento.
- La información no podrá ser compartida con terceros sin el previo consentimiento por escrito de Aliseda.
- El Proveedor deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y evite su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de la información almacenada y los riesgos a los que está expuesta.
- El Proveedor se compromete a colaborar en las investigaciones relacionadas con la seguridad de la información ante cualquier circunstancia: acciones legales, investigaciones forenses o cualquier tipo de requerimientos u actividades supervisoras o inspectoras de organismos y administraciones públicas.
- Cuando finalice la relación contractual por parte del Proveedor, éste estará obligado a devolver o destruir todo el material e información propiedad de Aliseda según determine el Departamento de Seguridad de la Información de Aliseda.

Auditoría

- Aliseda estará facultada para solicitar anualmente la compilación de un cuestionario, con el objetivo de valorar el nivel de cumplimiento del Proveedor con las medidas de seguridad internas.
- Aliseda, cumpliendo su capacidad de control sobre la información, podrá realizar por su cuenta revisiones de los sistemas de la información e instalaciones de tratamiento de información del Proveedor que verifiquen el cumplimiento de las políticas y medidas de seguridad de la información exigidas en el presente anexo y el contrato.
- En caso extraordinario, se podrá realizar una auditoría cuando se realicen modificaciones sustanciales en los sistemas de la información.
- Aliseda se reserva el derecho de solicitar cambios en los procesos de seguridad del Proveedor, si se consideran inadecuados. Estos cambios se deberán concordar recíprocamente, de manera razonable a nivel comercial y sujetos a tiempos aceptables.
- Gestión de incidentes de seguridad. El Proveedor tiene la obligación de comunicar inmediatamente a Aliseda cualquier incidente o brecha de seguridad que afecte directa o indirectamente a sus sistemas de información (el "Incidente") mediante el envío de un correo a seguridad.informacion@alisedainmobiliaria.com indicando: fecha del incidente, breve descripción del mismo, activos implicados e impacto para Aliseda, medidas adoptadas para su resolución.
- El Proveedor será responsable de realizar las acciones de contención y resolución de cualquier Incidente.
- A solicitud de Aliseda, el Proveedor informará pormenorizadamente de la resolución de Incidentes.

Clasificación y control de accesos

- El Proveedor debe crear, gestionar y mantener actualizado un registro documental de la información proporcionada por Aliseda.
- El Proveedor está obligado a trabajar con software verificado que no pueda acarrear riesgos adicionales a los datos de Aliseda.
- El Proveedor debe contar con procedimientos para realizar copias de seguridad y garantizar que después de un Incidente no se produzca una pérdida de la información.
- No se permite el almacenamiento de datos de Aliseda en dispositivos extraíbles (Pendrive, disco duro extraíble, etc.) a no ser que Aliseda lo autorice expresamente, en cuyo caso esta se deberá guardar cifrada.

Sistemas de Control de Acceso

- El Proveedor está obligado a mantener un registro actualizado y notificar a Aliseda los usuarios que dispongan de acceso a datos de Aliseda y su eventual cese en la asignación al servicio prestado a Aliseda.
- En caso de sustitución de responsables o usuarios, el Proveedor debe documentar la cancelación de las autorizaciones o accesos pertinentes.

- Los usuarios son únicos e intransferibles, por ello no está permitido que una persona comparta sus credenciales, excepto en aquellas aplicaciones, centros o entornos donde sea estrictamente necesario utilizar un usuario genérico o compartido (en cuyo caso existirá una persona responsable de la administración del usuario).
- Aliseda puede revisar cuando lo estime oportuno las autorizaciones de cada uno de los usuarios, pudiendo modificarlas o revocarlas.

Seguridad Ligada al Personal

- Es obligación del Proveedor proporcionar formación y concienciación en Seguridad de la Información (phishing, fuga de información…) al personal que da servicio a Aliseda.
- Los usuarios deberán aplicar las medidas necesarias para proteger el proceso de la información.
- El Proveedor garantiza que sus empleados tienen prohibido sacar la Información de Aliseda fuera de la propia organización, sin un permiso explícito del responsable de Seguridad de la Información de Aliseda.
    - Uso inadecuado de Internet que pueda suponer un riesgo para la información.
- El Proveedor garantiza que sus empleados conocen los riesgos y las precauciones con respecto a las descargas de ficheros o de código móvil de Internet.
- El Proveedor garantiza que cualquier persona asignada al servicio que cese en el mismo:
    - Devolverá y no custodiará ninguna información ni medios de Aliseda.
    - Todas las autorizaciones y accesos a los procesos de información de Aliseda son cancelados de manera inmediata.
- En caso de actuación indebida de cualquiera de los usuarios, el Proveedor deberá comunicarlo a Aliseda.

Comunicaciones y Gestión de Explotación

- Los equipos informáticos del usuario con los que trabaja el Proveedor dispondrán como mínimo de un sistema de antivirus actualizado, firewall local activado, cifrado del disco duro, contraseña de acceso al equipo, un sistema automático de cierre de sesión y de bloqueo de pantalla
- El Proveedor garantiza ser titular o tener licencia de todas las aplicaciones de software y sistemas informáticos que utilice para la prestación del servicio.
- Cuando el Proveedor acceda a los sistemas de Aliseda, su actividad y la de los usuarios podrá estar sujeta a seguimiento y monitorización en aspectos relacionados con la seguridad e integridad de la información.

Planes de Continuidad de negocio

- El proveedor deberá estar en disposición de continuar prestando el servicio de forma alternativa en caso de incidente que no permita el normal desarrollo de su actividad.

Control y gestión de los activos

- El Proveedor actualizará sus sistemas operativos y aplicaciones (estaciones de trabajo, servidores y equipos de telecomunicaciones) con las últimas actualizaciones de los parches de seguridad publicados por los fabricantes.

Normas de Seguridad Adicionales

Clasificación y control de accesos

- El Proveedor debe mantener un registro de accesos a la información durante toda la prestación del servicio y podrá ser requerido a efectos de control.
- No se harán pruebas de ningún tipo con datos reales, en caso necesario se deberá solicitar autorización al departamento de Seguridad de la Información de Aliseda.

Planes de Continuidad de negocio

- El Proveedor dispondrá de un Plan de Continuidad de Negocio actualizado en el que se contemple el servicio prestado a Aliseda y se garanticen los niveles de disponibilidad requeridos en los acuerdos de nivel de servicio incluidos en el contrato de prestación del servicio.
- El Proveedor tiene la obligación de identificar los posibles escenarios de desastres y deberá desarrollar un Plan de Recuperación ante Desastres ("DRP") ante los mismos y deberá ser testeado y actualizado como mínimo anualmente.
- Cualquier incidente que afecte a la Continuidad del negocio, se deberá notificar a Aliseda de manera inmediata, notificándolo a seguridad.informacion@alisedainmobiliaria.com.

Seguridad Física y del Entorno

- Las ubicaciones físicas que albergan sistemas de información deben estar protegidos contra accesos no autorizados y deben disponer de medidas de vigilancia y medidas de monitorización.
- Se dispondrá de sistemas de control de acceso a las zonas de seguridad, permitiendo identificar y registrar las personas que acceden a las mismas.
- Sólo podrá acceder a las zonas de Seguridad las personas autorizadas.

Control y Gestión de Activos

- Los sistemas de la información del Proveedor relacionados con Aliseda deben permanecer monitorizados continuamente y revisados desde una perspectiva de negocio.
- El Proveedor mantendrá actualizados sus sistemas operativos y aplicaciones (estaciones de trabajo, servidores y equipos de telecomunicaciones) con las últimas actualizaciones de seguridad disponibles.
- Todos los sistemas del Proveedor que estén relacionados con los sistemas de Aliseda deben estar monitorizados y actualizados con los parches de seguridad publicados por los fabricantes.
- El Proveedor establecerá y realizará procesos y procedimientos de gestión y ejecución de escaneos y gestión de vulnerabilidades.

Normas de Seguridad Adicionales Para Cumplir por los Proveedores que Desarrollen y/o mantengan Software para Aliseda

- Gestión de desarrollos: El Proveedor asegura que dispone de políticas de seguridad que indican explícitamente los requisitos y los procesos de seguridad a adoptar durante el desarrollo del software y de las aplicaciones, y acomodados a los estándares de seguridad comercialmente aceptados (OWASP, OSSTMM, etc.) y conformes con los requisitos normativos y de negocio aplicables. Asimismo, garantiza que dispone de un proceso de seguridad establecido, implementado y monitorizado durante el Ciclo de Desarrollo del Software (SDLC), que garantiza:
    - Que el desarrollo del software no contiene elementos que puedan comprometer la seguridad del sistema.
    - Que se respetan los criterios de seguridad suplementarios para la protección del software de ataques del tipo Cross Site scripting y SQL injection, entre otros, mediante los cuales se validan los datos de entrada y salida de la aplicación.
    - Que se adopta y aplica un proceso de modelado de amenazas, con un examen sistemático de las características y de los productos de la arquitectura, para identificar las amenazas y su mitigación.
    - Se aplican las 'mejores prácticas' de Seguridad en la validación de entrada, gestión de excepciones, etc.
    - Que las aplicaciones se proyectan en modo *load balancing* y *load monitoring* para prevenir la destrucción o indisponibilidad del servicio, a no ser que Aliseda decida otro tipo de arquitectura.
    - La integridad del propio código y la ausencia de "*backdoors*", realizando una declaración escrita cuando se consigna el software. Si la permanencia del Proveedor en el mercado no se puede garantizar a largo plazo, el Proveedor concederá en licencia el código fuente o lo depositará a terceros. El Proveedor debe proporcionar *patch* de seguridad para los productos desarrollados.
- El Proveedor garantiza la segregación física y lógica entre entornos de desarrollo, prueba y producción, y propondrá mecanismos asociados a servicios en red, controles de red y políticas de segregación de redes.
- El Proveedor garantiza que el proceso de subida a producción esté en todo momento controlado y aprobado por el usuario, y que durante dicho proceso se aplique una correcta segregación de funciones.
- El Proveedor restringirá el acceso al código fuente de las aplicaciones en entornos productivos a personal limitado e identificado, registrando la trazabilidad de las acciones que realizan.
- El Proveedor pondrá a disposición de Aliseda aquellos desarrollos de software hechos a medida por el Proveedor para Aliseda, incluyendo código fuente, código objeto, manuales o cualquier otra información relevante.
- El Proveedor garantizará que las librerías se mantienen actualizadas y libres de vulnerabilidades conocidas que puedan poner en riesgo todas las aplicaciones desarrolladas con las citadas librerías.
- En caso de que el Departamento de Seguridad de la Información encontrara incumplimientos de seguridad, se desarrollaría un plan para corregirlos en plazos acordados.

Las partes designarán un responsable de Seguridad de la Información. A tales efectos, se detallan a continuación los datos de contacto del responsable de Aliseda:

Por parte de Aliseda:

Nombre y apellidos: Juan José Canals Cugat Email: jjcanals@alisedainmobiliaria.com

Móvil: 608495870

Dirección: Avenida de Manoteras 12, 5ª Planta, 28050 Madrid