MANUAL DE TRATAMIENTO DE DATOS PERSONALES

Makler Inmobiliarios

NUESTRA
EMPRESA

Palacio Giraldo Grupo Inmobiliario nació con una finalidad muy clara: Ofrecer un acompañamiento a nuestros clientes en todos los procesos de gestióninmobiliaria, que pudiesen concreta se en experiencias de mejoramiento satisfacción, de quienes nos confiaron sus bienes o sus proyectos futuros inversión, con la promesa de asumir decisiones certeras que garantizaran y de un mejor futuro.

Continuando con esta finalidad y entendiendo las dinámicas del sector con losdesafíos que éstas nos imponen, hemos decidido crear nuestra marca Makler Inmobiliarios Más allá del cambio de nombre, estamos creciendo gracias a nuestro compromiso que ha generado confianza, a la calidad de recurso humano con el que contamos, a la formación de alto nivel de nuestros directivos, a la experiencia en todos los procesos de gestión inmobiliaria. Hoy contamos con todas las condiciones técnicas, con estándares de calidad y con el respaldo de La Lonja Propiedad Raíz de Medellín, nuestro aliado, y uno de los gremios de mayor trayectoria y reconocimientoen el Pais.

Por las razones expuestas tenemos la certeza de estar más preparados para ofrecer mayores y mejores servicios, con el renovado propósito de convertirnos en una empresa confiable para nuestros clientes, colaboradores y para el gremio inmobiliario en Medellín, en el País y en el extranjero. Bajo el lema de ofrecer siempre un servicio personalizado, integro y con altos estándares de calidad técnica y humana.

¡Crecemos para servirte mejor!

Makler Inmobiliarios

INTRODUCCIÓN

El presente manual tiene el propósito de definir los lineamientos para la implementación, monitoreo, sostenimiento y mejora continua del Programa de Protección de Datos Personales de MAKLER INMOBILIARIOS SAS, se toman como base los requisitos identificados en el estándar ISO/IEC 27001 en la ley 1581 de 2012, el decreto 1377 de 2013 y en ajuste a las instrucciones de la Circular Externa No. 02 del 3 de noviembre de 2015 EMITIDA POR LA SIC.

Las políticas incluidas en este manual se constituyen como parte fundamental del Modelo de Gestión de Seguridad de la Información de la Entidad y se convierten en la base para la implantación de los controles, procedimientos y estándares. La Seguridad de la Información es una prioridad para la empresa y por tanto es responsabilidad de todos los funcionarios velar por el continuo cumplimiento de las políticas definidas en el presente documento.

1 OBJETIVOS Y ALCANCE

1.1 Objetivo General

Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la Compañía, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Compañía, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes.

1.2 Objetivos Específicos

- Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.
- Establecer un modelo organizacional de Seguridad de la Información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.
- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todos los funcionarios y contratistas y demás personas que interactúen con la Compañía, para minimizar la ocurrencia de incidentes de Seguridad de la Información.
- Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

1.3 Alcance

El presente documento define la política, controles y directrices para el sistema de gestión de Seguridad de la Información de MAKLER INMOBILIARIOS S.A.S. La política establecida y sus posteriores actualizaciones aplican a todos los recursos y activos de información de la Compañía, así como a los designados para su uso y custodia.

2 MARCO NORMATIVO

2.1 Referencias Normativas

Con el propósito de dar un adecuado tratamiento a los datos personales, MAKLER INMOBILIARIOS S.A.S. ha identificado el siguiente marco normativo que articula las disposiciones de protección de los datos personales, su confidencialidad y los derechos de los titulares.

- Constitución Política de 1991: En su artículo 15 la Constitución establece lo siguiente: "(...) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (...)".

- Ley 1266 de 2008: Por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la provenientes de terceros países, y se dictan otras disposiciones.

- Ley 1273 de 2009 "Protección de la Información y de los Datos".

- Documento CONPES 3701 de Julio del 2011 "Lineamientos de política para ciberseguridad y ciberdefensa".

- Resolución No. 03049 del 24 de agosto de 2012, por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información.

- Ley 1581 de 2012: Por la cual se dictan las disposiciones generales para la protección de datos personales.

- Decreto Único 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se fijan estándares de un nivel adecuado de protección en el país receptor de la información personal

- Circular Externa 008 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se incluye un país en la lista de aquellos que cuentan con un nivel adecuado de protección de datos personales.

- Guía de la Superintendencia de Industria y Comercio para la implementación del Principio de Responsabilidad Demostrada (Accountability).

- En general, para la aplicación e interpretación del presente manual, cuando fuere procedente, se aplicarán las demás normas que regulen o complementen lo concerniente a la protección de datos personales.

3 PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS

MAKLER INMOBILIARIOS S.A.S. está comprometida con el adecuado tratamiento de los datos personales, por lo cual, en todas las actividades que tengan manejo de datos personales, se deberá garantizar la aplicación de los siguientes principios, los cuales se encuentran alineados con los establecidos en el artículo 4 de la Ley 1581 de 2012:

- **Legalidad:** En todo el proceso de tratamiento de los datos personales, desde el momento de su captura, almacenamiento y eliminación, se debe cumplir con las disposiciones normativas, empleando los datos para fines que estén bajo la ley y a las disposiciones reglamentarias que la desarrollen.

- **Finalidad:** Todos los datos personales que sean capturados en el desarrollo del ejercicio de las funciones educativas y administrativas que tiene MAKLER INMOBILIARIOS S.A.S, deben atender a finalidades específicas de acuerdo con el tratamiento que se le dará al dato. Las finalidades del tratamiento deben ser informadas a los titulares con el propósito que éstos conozcan las actividades que desarrollará la Empresa con los datos personales que está entregando.

- **Libertad:** La recolección, almacenamiento y tratamiento de los datos personales sólo puede realizarse con la autorización previa y expresa del titular, quien debe ser informado sobre el tratamiento que se les dará a sus datos personales. La divulgación o socialización de los datos personales sin la previa autorización, o sin una disposición legal que lo habilite, está prohibido.

- **Veracidad o calidad:** MAKLER INMOBILIARIOS S.A.S. debe promover que los datos personales que estarán sujetos a tratamiento deben ser veraces, exactos, completos y actualizados, pues de lo contrario pueden llevar a inducir a errores en la ejecución de tratamiento para el cual fueron capturados.

- **Transparencia:** Cualquier titular de información podrá tener acceso, en cualquier momento, a la información sobre sus datos personales tratados por MAKLER INMOBILIARIOS S.A.S.

- **Acceso y circulación restringida:** El tratamiento de los datos personales sólo podrá ser realizado por aquellos que el titular haya efectivamente autorizado, o por las personas habilitadas por las disposiciones legales vigentes.

- **Seguridad:** Toda la información asociada a los datos personales objeto de tratamiento por parte de MAKLER INMOBILIARIOS S.A.S, deberán protegerse bajo estándares de seguridad adecuados, implementando medidas operativas, técnicas y humanas que eviten su pérdida, adulteración o acceso no autorizado.

- **Confidencialidad:** MAKLER INMOBILIARIOS S.A.S. deberá garantizar la reserva de la información y datos personales que no estén bajo la categoría de datos públicos, por lo cual, todas las personas que tengan acceso al tratamiento de los datos personales deberán promover prácticas de manejo de datos que eviten su exposición o suministro a terceros no autorizados.

4 DISPOSICIONES GENERALES PARA LA OBTENCIÓN DE LA AUTORIZACIÓN

Toda captura, recolección, uso y almacenamiento de datos personales que realice MAKLER INMOBILIARIOS S.A.S, el desarrollo de sus actividades, y de aquellas finalidades dispuestas en la Política de Protección de Datos Personales, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.

Al efecto, la Empresa ha puesto a disposición de los titulares la autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la captura del dato, tanto de manera física como digital, a través de coberturas en modelos de autorizaciones o avisos de privacidad en donde se informa al titular sobre la captura de sus datos personales, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política de Protección de Datos Personales.

En todos los casos la obtención de la autorización se realizará bajo las diferentes modalidades que establece la ley, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información, y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, uno verbal o mediante una conducta inequívoca.

Es importante tener en consideración que en todos los casos MAKLER INMOBILIARIOS S.A.S debe custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Superintendencia de Industria y Comercio. Así las cosas, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento. La retención documental de las autorizaciones estará alineada con las Tablas de Retención Documental de la Empresa de acuerdo con el tipo de documento que las contiene o a las cuales están asociadas.

5 CONTENIDO DE LOS AVISOS DE PRIVACIDAD

De acuerdo con las disposiciones normativas, los avisos de privacidad mediante los cuales se obtiene la autorización de los titulares deben tener los siguientes elementos:

a) Nombre o razón social y datos de contacto del responsable del tratamiento
b) El Tratamiento al cual serán sometidos los datos y la finalidad de este.
c) Los derechos que le asisten al titular.
d) Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información.
e) En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

5.1 Autorización en Formatos

Los modelos de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web o documentos físicos.

5.1.1 Autorización en Formatos Web

Las áreas que, en el ejercicio de sus funciones, o debido a que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.

b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular.

c) El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.

d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.

e) Validar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas. Preferiblemente se deberá incluir fecha en la que se obtuvo la autorización.

5.2.2 Autorización en formatos físicos

Las áreas que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios físicos, deberán tener en cuenta los siguientes aspectos:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad.

b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento de los datos.

c) Para que la Universidad pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización. En el evento en que el titular no haya autorizado, deberá ser analizado de manera independiente.

d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos solicitados.

e) Garantizar la custodia de los formularios con sus respectivas autorizaciones.

5.3 Autorización en la toma de imagen (video y fotografías)

5.3.1 Autorización para Fotografías

Con el propósito de cumplir con las disposiciones legales para el tratamiento de datos privados como la imagen, MAKLER INMOBILIARIOS S.A.S ha dispuesto de avisos de privacidad con antelación a la toma.

Sin perjuicio de ello, la Empresa deberá velar por el adecuado cumplimiento de las directrices establecidas sobre protección de datos personales.

Dentro de las actividades que realiza MAKLER INMOBILIARIOS S.A.S están aquellas en las cuales participan terceros de quienes se puede capturar la imagen por video o fotografía. El área a cargo del tratamiento de los datos gestionará la autorización del titular para el uso de su imagen, garantizando su custodia.

5.4 Custodia de la autorización

Cada área de la Empresa que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos.

Así mismo, se deberán poner a disposición de la Superintendencia de Industria y Comercio o del Oficial de Protección de Datos en el evento en que éstos lo requieran.

6 RESPONSABILIDADES

- Verificar el cumplimiento del presente manual, en particular la difusión y adopción de las políticas, normas y estándares de Seguridad de la Información.
- Promover el desarrollo de una cultura de Seguridad de la Información a través de campañas de sensibilización y concientización.
- Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.
- Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con Seguridad de la Información.
- Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del sistema de gestión de Seguridad de la Información.
- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.
- Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de Seguridad de la Información.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Definir e implementar la estrategia de concientización y capacitación en Seguridad de la información para los funcionarios, contratistas y demás terceros, cuando aplique.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
- Gestionar la adquisición de Software y Hardware.
- Asignar los equipos de cómputo a los funcionarios y/o contratistas.
- Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información.

- Gestionar los incidentes de Seguridad de la Información que se presenten.

- Incluir en los programas de inducción y de re-inducción el tema de seguridad de la información asegurando que los empleados conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos.

- Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

7. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se describen algunas acciones identificadas que afectan la Seguridad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

1. Dejar los computadores encendidos en horas no laborables.

2. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.

3. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

4. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.

5. Hacer uso de la red de datos de la Empresa para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

6. Enviar información clasificada de la Empresa por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

7. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Empresa.

8. Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Compañía sin la debida autorización.

9. Usar servicios de internet en los equipos de la Compañía, diferente a los provistos.

10. Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario facilitar, prestar o permitir el uso de su cuenta personal a otro empleado o contratista.

11. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.

12. Retirar de las instalaciones de la Empresa computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.

13. Entregar, enseñar o divulgar información clasificada de la Compañía a personas o entidades no autorizadas.

14. Ejecutar acciones para eludir y/o modificar los controles establecidos en el presente manual.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

8. POLITICAS GENERALES

8.1 Concientización y Capacitación en Seguridad de la Información

a) La Empresa debe mantener un programa anual de concientización y capacitación para todos los empleados y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

b) Todos los empleados y contratistas al servicio de la empresa deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

8.2 Finalización de la Relación Laboral

Al momento de la desvinculación o cambio de roles en la Compañía, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

8.3 Derechos de Propiedad Intelectual

a) La empresa cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b) No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c) Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

d) El desarrollo de software a la medida adquirido a terceras partes o realizados por empleados de la empresa, serán de uso exclusivo de esta misma y la propiedad intelectual será MAKLER INMOBILIARIOS S.A.S.

8.4 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en el presente manual, conforme a lo dispuesto por las normas que rigen al personal de MAKLER INMOBILIARIOS S.A.S y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

13. Entregar, enseñar o divulgar información clasificada de la Compañía a personas o entidades no autorizadas.

14. Ejecutar acciones para eludir y/o modificar los controles establecidos en el presente manual.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

8. POLITICAS GENERALES

8.1 Concientización y Capacitación en Seguridad de la Información

a) La Empresa debe mantener un programa anual de concientización y capacitación para todos los empleados y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

b) Todos los empleados y contratistas al servicio de la empresa deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

8.2 Finalización de la Relación Laboral

Al momento de la desvinculación o cambio de roles en la Compañía, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

8.3 Derechos de Propiedad Intelectual

a) La empresa cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b) No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c) Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

d) El desarrollo de software a la medida adquirido a terceras partes o realizados por empleados de la empresa, serán de uso exclusivo de esta misma y la propiedad intelectual será MAKLER INMOBILIARIOS S.A.S.

8.4 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en el presente manual, conforme a lo dispuesto por las normas que rigen al personal de MAKLER INMOBILIARIOS S.A.S y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

9 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

Los usuarios que requieran usar los equipos fuera de las instalaciones de la empresa deben velar por la protección de los mismos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información del sector.

En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible, se deberá realizar inmediatamente el respectivo reporte a la Gerencia General y se deberá poner la denuncia ante la autoridad competente, si aplica.

10 POLÍTICAS DE ACCESO A LA RED

10.1 Gestión de Terceros

a) En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica y que deban desarrollarse dentro de las instalaciones de la Empresa, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar para el acceso a información sensible.

b) En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

c)Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

- Forma en los que se cumplirán los requisitos legales aplicables
- Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres
- Niveles de seguridad física que se asignará al equipamiento tercerizado.

10.2 Acuerdos de Confidencialidad

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo con el formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

10.3 Computación Móvil

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.

10.4 Administración de Contraseñas

Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

- Las contraseñas no deberán ser reveladas.

- Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento establecido.

- Los empleados y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones; las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones (Correo Electrónico, Orfeo, SIMA, etc); igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.

- Es deber de cualquier empleado y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

11 POLÍTICAS DE SEGURIDAD

11.1 Gestión de Activos de Información

I. La empresa tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.

II. La empresa debe identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.

III. La empresa debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

IV. Debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.

V. La Compañía deberá definir procedimientos para el rotulado y manejo de información de acuerdo con el esquema de clasificación definido.

11.2 Uso Adecuado de los Activos de Información

La información, los sistemas, las aplicaciones, los servicios y los equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) de todas y cada una de las dependencias y entidades de la empresa, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus respectivas actividades laborales. La empresa se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en la legislación vigente.

11.3 Uso de Internet

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

1) La navegación en Internet estará controlada de acuerdo con las restricciones de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

- Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

- Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.

- Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

- Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Empresa.

- Promover o mantener asuntos o negocios Empresa.

- Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.

- Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Empresa.

- Uso de herramientas de mensajería instantánea no autorizadas por la Empresa.

- Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

- Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

- El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

11.4 Uso del correo electrónico

La asignación de una cuenta de correo electrónico de la Compañía se da como herramienta de trabajo para cada uno de los funcionarios que la requieran para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

I. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas en la Compañía.

II. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Compañía y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

III. No se considera aceptado el uso del correo electrónico de la Compañía para los siguientes fines:

- Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

- Enviar mensajes no autorizados con contenido religioso o político.

- El envío de archivos adjuntos con extensiones o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Compañía.

IV. Toda información generada que requiera ser transmitida fuera de la Compañía, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

V. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.

VI. Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

- El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
- El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
- En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
- Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

11.5 Uso de Redes Inalámbricas

Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.

11.6 Uso de Recursos Tecnológicos

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo de los funcionarios y contratistas. El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la Compañía.
- Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.

11.7 Protección contra Software Malicioso

a) Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.

b) Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Empresa, y deberán ser actualizados permanentemente.

c) No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

d) La Empresa será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

e) Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

11.8 Administración de Backups, Recuperación y Restauración de la información

Se debe asegurar que la información definida como sensible y que se encuentra contenida en la plataforma tecnológica de la Compañía, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Es por esto por lo que las aplicaciones alojadas en los servidores de la Empresa se les realizarán copias de respaldo automáticas periódicamente.

Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
Para garantizar que la información de los funcionarios y contratistas sea respaldada, es responsabilidad de cada uno mantener copia de la información que maneja.

12 VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES

El Oficial de Protección de Datos Personales podrá, en cualquier momento, adelantar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos

personales, con el propósito de garantizar el adecuado cumplimiento y desarrollo del programa en la Empresa. Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas, los cuales tendrán seguimiento en los Comités de Habeas Data.

13 RESPONSABLES DE LA INFORMACIÓN

MAKLER INMOBILIARIOS S.A.S debe ser propietario legal de los activos de información. Ningún individuo puede reclamar los derechos de propiedad intelectual de un activo de información, a menos que se acuerde y apruebe por la Administración de acuerdo contractual.

Los usuarios están obligados por la política de uso aceptable de la organización.

- Usuarios externos, los empleados, terceros, Contratistas autorizado por el propietario / encargado de Acceso Y/o usuarios externos que hagan uso de la información sin que puedan modificarla, tratarla o borrar la información.

14 VIGENCIA

La presente política está vigente desde el 22 de enero del 2021.