DEFINICIONES

Las definiciones que se dan el marco de la legislación vigente y de las que haremos uso en este documento son:

A. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
B. Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.
C. Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
D. Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
E. Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
F. Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.
G. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
H. Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia del manual de políticas y procedimientos para el tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
I. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público.
   Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
J. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
K. Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la

información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. l. Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable

PRINCIPIOS

Los principios que VIVE TU aplica para el tratamiento de datos personales de los Titulares son:

A. a. Principio de legalidad en materia de Tratamiento de datos: El Tratamiento que VIVE TU dará a los datos personales en cuanto a su recolección, almacenamiento, uso,circulación y supresión de información se regirá por la legislación vigente referente a este tema.
B. Principio de finalidad: Se define la finalidad del tratamiento en este documento de acuerdo con la Constitución y la Ley, la cual será informada al Titular mediante este manual de políticas y procedimientos para el tratamiento de información.
C. Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, en ausencia de mandato legal o judicial que releve el consentimiento.
D. Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
E. Principio de transparencia: En el Tratamiento VIVE TU garantiza al titular el derecho al Titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
F. Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley.
   VIVE TU no mantendrá datos personales en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

G. Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. VIVE TU aplicará las medidas necesarias de seguridad para proteger la información personal de los Titulares en cumplimiento de las normas que sobre protección de datos personales le son exigibles y aquellas otras que sobre seguridad también le son aplicables en virtud del carácter de entidad sometida a control inspección y vigilancia de la Superintendencia Financiera de Colombia.
H. Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales en VIVE TU están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.
I. Principio de Confidencialidad y Tratamiento posterior: Todo dato personal que no sea Dato Público debe tratarse por los Responsables como confidencial, aun cuando la relación contractual o el vínculo entre el Titular del Dato Personal y la Compañía haya terminado. A la terminación de dicho vínculo, tales datos personales deben continuar siendo Tratados de conformidad con este manual de políticas y procedimientos para el tratamiento de información y con la Ley.
J. Principio de Temporalidad: VIVE TU no usará la información del Titular más allá del plazo razonable que exija la finalidad que fue informada al Titular.
K. Principio de Necesidad: Los Datos Personales solo pueden ser Tratados durante el tiempo y en la medida que el propósito de su Tratamiento lo justifique.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
Política Corporativa de Seguridad de la Información

En VIVE TU la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, VIVE TU implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el

cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en VIVE TU; este proceso será liderado de manera permanente por el Gerente General.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados Políticas generales de seguridad de la información VIVE TU ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de VIVE TU.
2. Los activos de información de VIVE TU, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
3. VIVE TU definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.
4. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
5. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.
6. Es responsabilidad de todos los funcionarios y contratistas de VIVE TU reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique
7. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.