LEY DE PROTECCIÓN DE DATOS

MANUAL INTERNO DE POLÍTICAS Y DE PROCEDIMIENTOS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

- **DLK S.A.S.**

DICIEMBRE DE 2016

TABLA DE CONTENIDO

I. INTRODUCCIÓN

Los lineamientos y reglamentaciones definidos en las leyes expedidas señalan el tratamiento que se debe realizar de la información personal de todo aquel que tenga relación con las empresas, sea cliente, proveedor o empleado de la misma, para el cumplimiento de las leyes y decretos reglamentarios, se establece el presente Manual de Políticas para el Tratamiento de Datos Personales, el cual contempla el manejo de solicitudes de aceptación, consultas y reclamos relacionados con el tratamiento de este tipo de información.

II. OBJETIVO

A través del presente documento, se establece el Manual Interno de Políticas y de Procedimientos para el Tratamiento de Datos Personales para la sociedad

El Manual Interno de Políticas y de Procedimientos para el Tratamiento de Datos Personales ha sido elaborado de acuerdo con los lineamientos señalados en la normatividad aplicable vigente sobre la materia. Y tendrá como alcance la aplicación a todas las bases de datos donde se almacene información personal y que sean objeto de tratamiento por parte de la sociedad.

III. ALCANCE

Estas políticas aplican para el tratamiento de la información personal de todos aquellos que tengan relación con LA EMPRESA, sean terceros (entre los que se incluyen clientes y proveedores) o empleados de la misma, de acuerdo a lo dispuesto por la ley.

IV. NORMATIVIDAD APLICABLE

Los aspectos más importantes para tener en cuenta según las leyes de protección de Datos en Colombia son: La Ley 1581 de 2012, el Decreto 1377 de Junio 27 de 2013, el Decreto 886 de 2014 y demás normas que las modifiquen, adicionen o complementen las cuales deben ser aplicadas en el DLK S.A.S

La Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia.

NOTA: En la medida que decreto(s) que incorpore(n) cambios que modifiquen las leyes anteriormente mencionadas, este Manual se ajustara de acuerdo a los cambios.

V. CONTENIDO DEL MANUAL INTERNO DE POLÍTICAS Y DE PROCEDIMIENTOS PARA EL TRATAMIENTO DE DATOS PERSONALES

1. Datos generales de la Empresa como responsable del tratamiento

2. Objetivos del Manual Interno de Políticas y de Procedimientos para el Tratamiento de Datos Personales

3. A quién se dirige Manual Interno de Políticas y de Procedimientos para el Tratamiento de Datos Personales

4. Ámbito de aplicación

5. Definiciones importantes en el tratamiento de datos

6. Principios rectores para el tratamiento de datos personales

7. Bases de Datos

8. Autorización del titular para el tratamiento de datos

9. Autorización del titular para el tratamiento de datos sensibles

10. Uso y finalidad del tratamiento de datos personales

11. Aviso de privacidad

12. Revocatoria de la autorización y/o supresión del Dato

13. Derechos de los titulares de los datos.

14. Procedimiento para el ejercicio de los derechos como titular del dato

15. Deberes de la Empresa como responsable del tratamiento

16. Medidas de Seguridad aplicadas al tratamiento de las bases de datos

17. Dependencia encargada del trámite para que el titular de los datos ejerza sus derechos de peticiones, consultas y reclamos.

18. Modificación de la política de tratamiento

19. Entrada en vigencia de la política de tratamiento

VI. POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

1. Datos generales de la Empresa como responsable del tratamiento de Datos Personales

Razón Social:

- DLK S.A.S

El presente Manual incluirá la sociedad anteriormente mencionada.

- NIT. 800.095.036 – 4

Domicilio: Carrera 14 86ª 45, Bogotá – Colombia

Ciudad: Bogotá

Teléfono: 571- 3 77 92 69

Página web:

Las páginas web de la empresas son las siguientes:

- http://www.diluccatogo.com
- http://www.dlkrestaurantes.com

2. Objetivos del Manual de Políticas de Tratamiento de Datos Personales

El presente Manual tiene por objeto proteger el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos de propiedad de la **DLK S.A.S,** o cuyo tratamiento ha sido encargado al **DLK S.A.S**, en desarrollo y cumplimiento de su objeto social, así como los demás derechos, libertades y garantías constitucionales a que se refieren los artículos 15 (derecho a la intimidad) y 20 (derecho a la información) de la Constitución Política de Colombia.

En este Manual de Políticas de Tratamiento de Datos Personales usted encontrará los lineamientos legales y corporativos bajo los cuales el **DLK S.A.S,** realiza el tratamiento de sus datos, la finalidad, sus derechos como titular, así como los procedimientos internos y externos que existen para el ejercicio de tales derechos ante el **DLK S.A.S,.**

La empresa **DLK S.A.S,** entienden por protección de datos todas aquellas medidas tomadas a nivel físico, técnico y jurídico para garantizar que la información de los Titulares – personas naturales - (proveedores, personal de la empresa **DLK S.A.S,** empleados, ex empleados, clientes, etc.) registrados en la base de datos de la empresa **DLK S.A.S,** esté segura de cualquier ataque o intento de acceder a ella por parte de personas no autorizadas, así como que su uso y conservación sea adecuado a la Finalidad establecida para la recolección de los Datos Personales.

Este Manual tiene como objetivo dar cumplimiento a la legislación vigente en materia de protección de datos, en especial a la Ley 1581 de 2012, al Decreto 1377 de 2013, al Decreto 886 de 2014, a la Resolución 886 de 2014 (y a las demás normas que los modifiquen, adicionen, complementen o desarrollen).

3. A quién se dirige la política de tratamiento de datos personales

La presente Política de Tratamiento de Datos Personales está dirigida todas las personas naturales que tengan o hayan tenido alguna relación con la empresa **DLK S.A.S**, a saber, empleados, ex empleados, clientes, proveedores, tanto activos como inactivos o cualquier tercero cuyos Datos Personales se encuentran incluidos en las Bases de Datos de **DLK S.A.S**

4. Ámbito de aplicación

El ámbito de aplicación de este Manual de conformidad con la Ley 1581 de 2012, serán los datos de personas naturales registrados en todas las base de datos de propiedad de la empresa **DLK S.A.S**, o cuyo tratamiento ha sido encargado a éstas.

El presente Manual aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando la empresa **DLK S.A.S,** en su calidad de Responsable o Encargado del Tratamiento de los Datos, dejare de estar domiciliada en el territorio nacional, más sin embargo, le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en el presente Manual no será de aplicación de:

a) Las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas Bases de Datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la ley de Habeas Data.

b) Las Bases de Datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

c) Las Bases de Datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

d) Las Bases de Datos y archivos de información periodística y otros contenidos editoriales.

e) Las Bases de Datos y archivos regulados por la Ley 1266 de 2008.

f) Las Bases de Datos y archivos regulados por la Ley 79 de 1993.

5. Definiciones importantes en el tratamiento de los datos

Para la interpretación de las políticas y aplicación a las reglas contenidas en este Manual, le pedimos tener en cuenta las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Aviso de Privacidad**: Comunicación verbal o escrita generada por el Responsable (siendo el responsable la sociedad DLK S.A.S), dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de 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.

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

- **Causahabientes de los datos:** persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero)

* **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Dato Privado:** El dato privado es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato Semiprivado**: El dato semiprivado es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector personas o a la sociedad en general, como el dato financiero y crediticio.

- **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 y a 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.

- **Datos Sensibles:** Aquellos datos 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.

- **Datos Biométricos:** Son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población como Huellas dactilares, Análisis del ADN.

- **Empleado:** Persona natural que en virtud de un contrato de trabajo se obliga a prestar un servicio personal a otra persona natural o jurídica, bajo la continuada dependencia o subordinación de la segunda y mediante remuneración.

- **Ex empleado:** Persona natural que estuvo vinculada laboralmente con **LA EMPRESA**.

- **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.

- **DLK S.A.S:** Sólo para efectos de este documento, DLK S.A.S incluye en el Anexo No. 1 de este documento se menciona la titularidad que se encuentra en cabeza de la sociedad anteriormente mencionada.

- **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.

- **Política de Tratamiento:** Se refiere al presente documento, como política de tratamiento de datos personales aplicada por **LA EMPRESA** de conformidad con los lineamientos de la legislación vigente en la materia.

- **Proveedor / Marca:** Para los efectos de este documento, toda persona natural o jurídica que preste algún servicio a **LA EMPRESA** en virtud de una relación contractual.

- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento, sea empleados, ex empleados, proveedores, clientes tanto activos como inactivos de **LA EMPRESA** o cualquiera que suministre datos personales a **LA EMPRESA**.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

• **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.

• **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. **Visitante**: persona (s) que están en un lugar por una duración inferior a 8 horas sin ejercer una actividad que se remunere en el lugar visitado.

6. Principios rectores para el tratamiento de datos personales

La Ley 1581 establece en el Artículo 4 que los siguientes principios son rectores del Tratamiento de sus Datos Personales y que la empresa **DLK S.A.S**, como entidades respetuosas de la ley acatarán: • **Principio de Legalidad:** El Tratamiento de los datos personales es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 de 2012 en el Decreto 1377 de 2013 y en las demás disposiciones que las desarrollen. • **Principio de Finalidad:** El Tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular. • **Principio de Libertad:** El Tratamiento de los datos personales sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. • **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. • **Principio de Transparencia**: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. • **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 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 ley. Los datos personales, salvo la información pública, no podrán estar disponibles 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 conforme a la ley. • **Principio de Temporalidad del dato:** agotada la finalidad para la cual fue recolectado y/o tratado el dato personal, el responsable o encargado cesará su uso**. Principio de Seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, 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. • **Principio de Confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos 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 ley y en los términos de la misma.

Deber de información: la empresa **DLK S.A.S** informará a los titulares de los datos personales, así como a los responsables y encargados del tratamiento, del régimen de protección de datos adoptado, así como la finalidad y demás principios que regulen el tratamiento de esos datos. La empresa **DLK S.A.S** informará además sobre la existencia de las bases de datos de carácter personal que custodien, los derechos y el ejercicio del habeas data por parte de los titulares procediendo al registro que exige la ley

7. Bases de Datos

7.1. Bases de Datos en las que la empresa DLK S.A.S actúa como responsable y encargada del tratamiento:

En el Tratamiento de los datos contenidos en las siguiente Base de Datos, la empresa **DLK S.A.S** actúa tanto en calidad de "**Responsables**", toda vez que son quienes recaudan la información y toman las decisiones sobre el Tratamiento de los datos, como en calidad de "**Encargadas**", en la medida en que son quienes realizan el Tratamiento de los datos.

A continuación se mencionan las 4 Bases de Datos sobre las cuales la empresa **DLK S.A.S** realiza tratamiento de información personal:

7.1.1. Base de Datos de Proveedores

Descripción

Esta base de datos corresponde a la información personal que se recolecta sobre las personas naturales proveedores de bienes y servicios que ofrecen, prestan servicios o venden productos a la empresa DLK S.A.S

Contenido

Esta base de datos contiene la siguiente información: nombre de la persona, el número de identificación, el teléfono, el correo electrónico, la dirección de contacto, la persona de contacto, la actividad económica, la información financiera, referencias comerciales, referencias personales, contratos realizados con otros terceros, el régimen y datos necesarios para cumplir con la finalidad de esta base de datos..

Forma en que se recopilan los datos

La información primordialmente se obtiene a través del formato de creación de terceros. En este formato el proveedor autoriza para verificar la información suministrada, reportar, almacenar, actualizar, consultar, procesar, compilar, intercambiar, suministrar, grabar, solicitar y divulgar la información de carácter personal ante cualquier operador, centrales de información del Sector Financiero con fines estadísticos, de control, supervisión,

pruebas de mercadeo, actualización o verificación información de conformidad con lo preceptuado en la ley de habeas data y de protección de datos personales.

Finalidad

La información contenida en esta base de datos tiene por finalidad crear al proveedor en el sistema de la empresa DLK S.A.S., cumplir con las obligaciones derivadas del contrato comercial, realizar pagos, realizar transferencias bancarias asociadas a los servicios prestados a la empresa DLK S.A.S, llevar un control de los proveedores, facturar los servicios o productos adquiridos, llevar control de pagos y de niveles de compras, enviar reportes a DIAN, y a la Secretaria de Hacienda Departamental y en general entidades tributarias, de conformidad con lo dispuesto en la normatividad colombiana. Igualmente, es utilizada para contactarlos para contratar de nuevo.

La Base de Datos de Proveedores también puede ser utilizada para dar cumplimiento a las obligaciones contraídas con proveedores así como evaluar la calidad de productos y servicios.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, de procesamiento, de almacenamiento y de uso.

Para DLK S.A.S el área responsable de esta información es el área de Contabilidad. Esta información se encuentra contenida en las instalaciones de la Cabrera, en los Sistemas Siigo, Aldelo, Gamasab y en carpetas físicas.

Los proveedores titulares de la información personal, han dado autorización a la empresa DLK S.A.S. para verificar la información suministrada, así como para reportar, almacenar, actualizar, consultar, procesar, compilar, intercambiar, suministrar, grabar, solicitar y divulgar la información de carácter obtenida a Centrales de Información con fines estadísticos, de control, supervisión, pruebas de mercadeo, actualización o con fines de verificación de información de conformidad con lo preceptuado en la ley de habeas data. De manera tal que con esta autorización, la información puede ser compartida con Centrales de Información.

Sobre las medidas de **seguridad**, la empresa DLK S.A.S han previsto códigos de acceso y usuarios restringidos que sólo pueden consultar esta información. De manera tal que sólo los usuarios que crean la información tienen permiso para su uso, es decir las áreas de Compras, de Impuestos y de Contabilidad.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

Esta base de datos se encuentra vigente mientras exista la relación comercial con el proveedor más un periodo adicional de 10 años. Así mismo se conserva un archivo histórico de los proveedores que han estado vinculados con DLK S.A.S. Es importante

tener presente que DLK S.A.S cuenta con una Política de Archivo. De manera tal que la temporalidad de esta base de datos es concordante con la Política de Archivo.

7.1.2. Base de datos del personal de la empresa (empleados):

Descripción:

Esta Base de Datos contiene la información que se recolecta sobre los empleados y contratistas (vinculados a través de contratos de trabajo y de prestación de servicios), estudiantes en práctica y aprendices del Servicio Nacional de Aprendizaje SENA y es manejada por el Área de Talento Humano de la empresa DLK S.A.S.

Contenido:

La información personal contenida en esta Base de Datos contiene los siguientes datos personales: nombre, apellidos, cédula de ciudadanía, fecha y lugar de expedición, fecha y lugar de nacimiento, edad, sexo, estado civil, lugar de residencia, dirección, teléfono fijo y celular, ciudad, sueldo, fecha de ingreso, fecha de examen médico, AFP, EPS, AFC, los datos de familiares incluidos los niños, niñas y adolescentes en el primer grado de consanguinidad es suministrada por los colaboradores directamente por medio de la Intranet (módulo de autogestión), datos de registro biométrico (Huella) es suministrada por el área administrativa y algunos punto de venta en prueba, cargo, nivel de estudios, los datos de la persona a contactar en caso de emergencia se maneja en la carpeta del colaborador en los puntos de venta la relacionan, número de cuenta bancaría para nómina, entidad bancaria y ciudad.

La empresa también recopila los siguientes datos sensibles: Grupo Sanguíneo, información que es suministrada por los colaboradores directamente por medio de la intranet (Módulo de Autogestión).

Forma en que se recopilan los datos

El Área de Desarrollo Humano recoge la información contenida en esta base de datos del proceso de contratación de personal, de la hoja de vida y del examen médico. Los Datos son solicitados a los Titulares a través del Contrato laboral o de prestación de servicios.

Finalidad

Los datos anteriormente mencionados únicamente se recopilan con el fin de cumplir con las obligaciones derivadas del contrato laboral, dentro de los que están, la atención de solicitudes, la generación de certificados y constancias, la afiliación a las entidades del Sistema de Protección Social, la realización de actividades de Bienestar Laboral, el levantamiento de registros contables, los reportes a autoridades de control y vigilancia, la adopción de medidas tendientes a la prevención de actividades ilícitas, pagar impuestos, comunicación en caso de ausencia, entre otros fines administrativos, comerciales y de contacto.

Los datos sensibles como la huella, se utilizan para el pago de la nómina de personal operativo y el grupo sanguíneo u otra información relacionada con la salud del trabajador, se utiliza en casos de emergencia, o para el reporte ante las entidades del Sistema de Seguridad Social en Salud.

Tratamiento

El tratamiento que recibe esta base de datos por parte de LA EMPRESA en su condición de responsable y encargada incluye la recolección, el almacenamiento y el uso. Los datos también son utilizados para enviar reportes a las entidades administrativas que lo soliciten, con base en las normas del Sistema de Seguridad Social y complementarias. Los datos de empleados se encuentran contenidos en físico en las instalaciones de La cabrera y en el Sistema Siigo.

En cuanto a las medidas de seguridad, la información personal contenida en esta base de datos sólo la puede consultar quien la crea y quien tiene permiso para uso, es decir el área de Talento Humano.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

Esta Base de Datos estará vigente mientras exista la relación laboral entre el empleado y LA EMPRESA, y por diez (10) años más contados a partir de la fecha de liquidación del contrato. Sin embargo, para asuntos de aportes a pensiones LA EMPRESA conservar en archivo esta información mínimo por 90 años. Así mismo LA EMPRESA conserva la información en un archivo histórico de las personas que han estado vinculadas a LA EMPRESA.

7.1.3. Base de datos de clientes:

Descripción

Esta base de datos corresponde a la información de los clientes de la empresa **DLK S.A.S** quienes adquieren los diferentes bienes y servicios.

Contenido

Esta base de datos contiene la siguiente información personal: nombre, identificación, teléfono, Correo electrónico, número de Celular, dirección y domicilio.

Forma en que se recopilan los datos

La información se obtiene a través de los siguientes medios:

Por las Páginas web de **DLK S.A.S:**

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

- A través del formato de creación de terceros

- Por teléfono.

Finalidad

La información contenida en esta base de datos tiene por finalidad permitir a LA EMPRESA cumplir apropiadamente con su objeto de venta de alimentos y bebidas y prestar un buen servicio.

La información personal de clientes obtenida por DLK S.A.S tiene por finalidad atender el despacho de pedidos a través del Call Center, al igual que para quejas o preguntas.

Adicionalmente, esta base de datos se utiliza para dar cumplimiento a obligaciones contraídas con clientes, evaluar la calidad de productos y servicios, informar sobre nuevos productos o servicios relacionados, y llevar a cabo campañas, promociones o concursos de carácter comercial o publicitario. Esta base de datos también se utiliza para información comercial, publicitaria o promocional sobre los productos y/o servicios, eventos y/o promociones de tipo comercial.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, de procesamiento, de almacenamiento y de uso. Para los casos de consulta se recolecta y almacena.

La autorización se obtiene en La Taqueria con la aceptación de términos en la página web, o la autorización se obtiene a través del Call Center y queda grabada. Quienes han suministrado sus datos en la página web, han otorgado autorización con la aceptación de términos en la página.

Sobre las medidas de **seguridad**, se tienen mecanismos y herramientas para que sólo pueda consultar la información quien la crea y quien tiene permiso para uso.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

La información personal contenida en esta base de datos es custodiada mientras dura la relación comercial con el cliente más un periodo adicional de 10 años.

Si en un caso individual, existen indicios de una necesidad de protección o de interés histórico de estos datos, se prolongará el plazo de almacenamiento de estos datos hasta que se haya aclarado la necesidad legal de protección.

7.1.4. Base de Servicio al Cliente (PQRF)

Descripción

Esta base de datos corresponde a la información de los clientes de la empresa **DLK S.A.S** quienes hacen uso de diferentes canales de servicio al cliente.

Contenido

Esta base de datos contiene la siguiente información personal: nombre teléfono, celular, caso de incidencia presentada, punto de venta, coordinador encargado del punto de venta y acciones a tomar.

Forma en que se recopilan los datos

La información de esta base de datos se obtiene a través de las redes sociales Facebook y Twitter. Al respecto, es importante tener en cuenta que, con el acceso a estas redes sociales y a través de sus políticas de uso, los titulares aceptan los términos y condiciones de uso y de privacidad, en las cuales se reconoce que su voluntad precisamente compartir la información en redes sociales. De manera que se trata de conductas inequívocas de los titulares, que constituyen una forma tácita de otorgar autorización.

En efecto, los términos y condiciones establecidos en Twitter establecen que los titulares de los datos personales autorizan a la red social a utilizar su información, y por lo tanto a transferirla y almacenarla en el país en los que operan. Por su parte, las políticas de privacidad de Facebook establecen que los titulares son propietarios de todo el contenido y la información que publican en la red social y controlan cómo se comparte a través de la configuración de la privacidad y de las aplicaciones. De manera que la información obtenida en redes sociales, al ser una información cuyo titular quiso que se hiciera pública, si sólo es utilizada en las redes sociales no requiere autorización de su titular. Sin embargo si la información se extrae y se construye una base de datos sí requiere de autorización previa y expresa de su titular.

1 Twitter establece que sus servicios están principalmente diseñados para ayudar a sus usuarios a compartir información con el mundo, pues la mayoría de la información que los titulares facilitan a través de los Servicios de Twitter es información que el titular pide que se haga pública. Esta información incluye los mensajes twitteados; los metadatos facilitados con los Tweets el idioma, el país y la zona horaria asociados a su cuenta; las listas que crea, las personas a las que sigue, los Tweets que retwittea o marca como Me gusta, y demás informaciones que se generan mediante el uso de los Servicios de Twitter. Adicionalmente Twitter advierte que cuando comparta información o contenidos como

fotografías, videos y enlaces a través de los Servicios, debería reflexionar cuidadosamente sobre aquello que está publicando.

La información también se obtiene a través de las páginas web de la empresa:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

El área de Servicio al Cliente es la encargada del tratamiento de la información de esta base de datos al interior de LA EMPRESA.

Finalidad

La información contenida en esta base de datos tiene por finalidad hacerle seguimiento y atención a las peticiones, quejas y reclamos del cliente. Asimismo, la finalidad de esta base de datos es generar estadísticas internas de servicio al cliente.

Esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, procesamiento, almacenamiento, uso y circulación interna.

Cada cadena tiene un formulario, (a través de las plataformas de contáctanos, háblanos y trabaja con nosotros), el cual llega a una plataforma coordinada por el Área de Servicio al Cliente. La respectiva área descarga y alimenta esta base de datos.

El área de Servicio al Cliente tiene acceso a esta base de datos y la comparte internamente con los coordinadores.

La información es custodiada en un computador al cual tiene acceso el respectivo funcionario bajo un sistema de ingreso por claves. Esta base de datos es utilizada en las áreas de cada de departamento para fines estadísticas, de gestión y para los demás fines indicados en el numeral anterior.

Estos datos son intransferibles y confidenciales.

Sobre las medidas de seguridad, los datos sólo son manejados por el personal de la EMPRESA y nadie ajeno a la misma tiene acceso a estos datos de manera que la seguridad se garantiza mediante directorio activo de Windows para uso de lectura o modificación por grupos de usuario o usuarios. Así las cosas, la información se garantiza a través de medidas de seguridad de claves de computadores de las áreas o funcionarios autorizados, así como claves y roles de los sistemas de información así como la segregación de roles y perfiles.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

Esta base de datos ha venido siendo recopilada desde el mes de junio del año 2016 y estará vigente por el término de 6 años siguientes a la fecha del registro individual del dato personal. Si en un caso individual, existen indicios de una necesidad de protección o de interés histórico de estos datos, el plazo de almacenamiento de estos datos se prolongará hasta que se haya aclarado la necesidad legal de protección.

Adicionalmente y dado que la EMPRESA cuenta con una Política de Archivo, la temporalidad de esta base de datos es concordante con la Política de Archivo.

7.2. Bases de Datos en las que se recolectan Datos Especiales

7.2.1. Bases de datos Sensibles

Para los efectos del manejo de los Datos Sensibles, **LA EMPRESA** ha obtenido la correspondiente autorización de los Titulares cuya información reposa en sus Bases de Datos y obtendrá la autorización de manera previa, siempre que se trate de nuevos datos.

Para el tratamiento de los datos sensibles **LA EMPRESA** ha cumplido con las siguientes obligaciones:

- Informó al Titular que por tratarse de Datos Sensibles, no estaba obligado a autorizar su tratamiento.

- Informó al Titular cuáles de los datos son Sensibles y la finalidad del Tratamiento.

- **LA EMPRESA** no condiciona ninguna actividad a que el Titular suministre Datos Sensibles.

7.2.2. Base de Datos Personal

Esta base de datos se encuentra descrita en el numeral 7.1.1 del presente Manual.

7.3. Registro de las bases de Datos

De conformidad con lo dispuesto en el Decreto 886 de 2014 las bases de datos anteriormente mencionadas serán inscritas en el Registro Nacional de Base de Datos.

8. Autorización del titular para el tratamiento de datos

De acuerdo al artículo 5 del Decreto 1377 de 2013, **LA EMPRESA** como Responsable del Tratamiento ha elaborado un formato de **"Autorización para el Tratamiento de Datos Personales"** y ha adoptado procedimientos para solicitarle, a más tardar en el momento

de la recolección de sus datos personales, su autorización para el Tratamiento de los mismos e informarle cuáles son los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene su consentimiento.

Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, pueden ser tratados por **LA EMPRESA**, siempre y cuando, por su naturaleza, sean Datos Públicos.

Se entenderá que la autorización otorgada por el Titular a **LA EMPRESA**, cumple con los requisitos exigidos en la legislación vigente aplicable, cuando ésta se manifieste: • Por escrito • De forma oral • Mediante conductas inequívocas del Titular que permitan concluir de forma razonable que éste otorgó a **LA EMPRESA** la autorización respectiva. En ningún caso su silencio será asimilado por **LA EMPRESA** como una conducta inequívoca.

LA EMPRESA ha establecido canales para que el Titular de los datos, pueda en todo momento solicitar como Responsable o Encargado del Tratamiento, la supresión de sus datos personales y/o revocar la autorización que nos ha otorgado para el Tratamiento de los mismos.

9. Autorización del titular para el tratamiento de los datos sensibles

En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el Artículo 6 de la Ley 1581 de 2012, **LA EMPRESA** cumplirá con las siguientes obligaciones:

9.1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.

9.2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad de su Tratamiento, y además obtener su consentimiento expreso.

Ninguna de las actividades que realiza **LA EMPRESA** está ni estará condicionada a que el titular suministre sus datos personales sensibles.

10. Uso y finalidad del tratamiento de datos personales

LA EMPRESA como entidad respetuosa de la privacidad de las personas reconoce que el Titular de los datos personales tiene derecho a contar con elementos adecuados que garanticen la misma, teniendo en todo caso para ello en cuenta sus responsabilidades, derechos y obligaciones.

En virtud de la relación que se ha establecido o se establezca entre el Titular de los datos personales y **LA EMPRESA**, es importante que este conozca que **LA EMPRESA** recolecta, registra, almacena, usa los datos personales de los Titulares, para su propio uso con los propósitos que fueron solicitados o por requerimientos de las entidades públicas.

Los Datos Personales de los Titulares son utilizados por **LA EMPRESA** para: • Ejecutar las actividades propias de **LA EMPRESA** para cumplir su objeto social, todo lo cual se hará con base en la finalidad de la Base de Datos en la que reposan los Datos Personales de los Titulares. • Ofrecerle los productos, servicios y o beneficios que buscan satisfacer las necesidades de los Titulares, o los productos y servicios de **LA EMPRESA**, lo cual puede hacerse por medios físicos o a través de correos electrónicos y/o terminales móviles. • Enviar la información a entidades gubernamentales por exigencia legal. • Consultar información en las listas de control (Listas Nacionales e Internacionales), consultar a la CIFIN, a las centrales de información, Lista Clinton, Procuraduría, Contraloría, Policía Nacional, DIJIN con el fin de preservar la confianza y transparencia entre el Titular de los Datos y **LA EMPRESA** • Soportar procesos de auditoría externa e interna. • Para la ejecución de procesos de índole judicial y extrajudicial en los casos permitidos por los Estatutos y Reglamentos de **LA EMPRESA**. • Registrar la información de Empleados, ex empleados, proveedores, clientes (activos e inactivos) en las bases de datos de **LA EMPRESA**, para el envío de información contractual, comercial y obligacional a que hubiere lugar. • Para verificación de referencias de empleados, ex empleados, proveedores, clientes (activos e inactivos) en las bases de datos. • Respecto de la recolección y tratamiento de datos realizados mediante mecanismos automatizados con el objeto de generar registros de actividad de los visitantes y registros de audiencia **LA EMPRESA**, sólo podrá utilizar dicha información para la elaboración de informes que cumplan con los objetivos señalados. En ningún caso podrá realizar operaciones que impliquen asociar dicha información a algún usuario identificado o identificable.

Los Datos Personales serán utilizados por **LA EMPRESA** sólo para los propósitos aquí señalados, por lo tanto, **LA EMPRESA** no venderá, licenciará, transmitirá o divulgar los Datos Personales, salvo que: • El Titular autorice expresamente a hacerlo • La información del Titular tenga relación con una fusión, consolidación, adquisición, desinversión u otro proceso de restructuración de **LA EMPRESA** • Sea permitido por la ley.

Para el manejo interno de los Datos, éstos podrán ser conocidos por el personal autorizado de **LA EMPRESA,** lo cual incluye la Asamblea General de Accionistas, la Junta Directiva, la Revisoría Fiscal, la Presidencia, las Vicepresidencias y las Gerencias.

LA EMPRESA podrá subcontratar a terceros para el procesamiento de determinadas funciones o información. Cuando ello ocurra, dichos terceros estarán obligados a proteger los Datos Personales en los términos exigidos por la ley y en su condición de Encargados del manejo de las Bases de Datos de **LA EMPRESA**.

En el caso de transmisión de datos personales, **LA EMPRESA** suscribirá el contrato de transmisión a que haya lugar en los términos del Decreto 1377 de 2013.

Igualmente, **LA EMPRESA** podrá transferir o transmitir (según corresponda), guardando las debidas medidas de seguridad, los datos personales a otras entidades en Colombia o en el extranjero para la prestación de un mejor servicio, de conformidad con las autorizaciones que hayan sido otorgadas por los Titulares de los datos personales.

Una vez cese la necesidad de Tratamiento de los Datos Personales, los mismos serán eliminados de las bases de datos de **LA EMPRESA** en términos seguros.

11. Aviso de Privacidad

Esta leyenda se encuentra impresa en todos los formularios o documentos por medio de los cuales se recolecta información de los proveedores, trabajadores, clientes y demás titulares de los datos personales que maneja **LA EMPRESA**. Cuando se recolectan de manera verbal, esta leyenda es comunicada al Titular de igual forma, y de la autorización se deja constancia a través de medios técnicos dispuestos para el efecto.

Aviso de Privacidad:

LA EMPRESA declara que protege los datos personales suministrados por los titulares en virtud de lo dispuesto en la Ley 1581 de 2012 e informa a éstos que los datos personales serán utilizados en los términos dados en la autorización por el titular del dato.

2 En el aviso de privacidad se incluirá el nombre de la empresa DLK S.A.S que corresponda

Los datos personales suministrados por el Titular serán utilizados por **LA EMPRESA** para los fines previstos en el Manual Interno de Políticas y Procedimientos para el Tratamiento de Datos Personales.

Los datos serán objeto de recolección, almacenamiento, actualización, y copia de seguridad **de conformidad con lo previsto en el Manual Interno de Políticas y Procedimientos para el Tratamiento de Datos Personales**.

El Responsable y Encargado del Tratamiento de los datos será la empresa **DLK S.A.S.** El tratamiento podrá realizarse directamente por LA EMPRESA o por el tercero que esta determine.

Vigencia de los datos: Los datos personales suministrados por los Titulares se mantendrán almacenados de acuerdo con lo dispuesto en el Manual Interno de Políticas y Procedimientos para el Tratamiento de Datos Personales. 26

El Titular tiene derecho a conocer, actualizar, rectificar, revocar, solicitar la supresión, presentar quejas y reclamos y demás derechos contenidos en la ley 1581 de 2012 y sus Decretos Reglamentarios, respecto de los datos suministrados.

El titular puede conocer el Manual Interno de Políticas y Procedimientos para el Tratamiento de los Datos de **LA EMPRESA** a través de los siguientes links:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

Los datos de contacto de **LA EMPRESA** son: teléfono: 571-3779269 en la ciudad de Bogotá, correo electrónico: servicioalcliente@dlksa.net, servicioaalcliente@dilucca.com, Dirección: Carrera 14 86a 45, Bogotá – Colombia, Dependencia Encargada : Área de Servicio al Cliente.

Autorización:

Para la página web:

LA EMPRESA declara que protege los datos personales de conformidad con lo dispuesto en la Ley 1581 de 2012.

Con la aceptación de esta autorización usted declara que todos los datos aquí contenidos son exactos y veraces. Los datos personales suministrados por Usted son utilizados por LA EMPRESA para la venta y prestación de nuestros servicios, atender peticiones, evaluar la calidad de sus productos y servicios, información comercial sobre nuevos productos o servicios, llevar a cabo campañas publicitarias, promociones o concursos de acuerdo con su Política de privacidad que podrá ser consultada en el siguiente POLITICA DE TRATAMIENTO DE DATOS PERSONALES.

A través de esta aceptación usted manifiesta haber leído y comprendido la Política de Tratamiento de Datos Personales de la EMPRESA y por ende, acepta libremente el tratamiento que se le dará a sus datos personales, que incluye almacenar, procesar, disponer, así como transferir dichos a las personas naturales o jurídicas de acuerdo con las finalidades y condiciones mencionadas en la Política de Privacidad.

Firma_____ Fecha:_____

Guión de telemercadeo:

Esta llamada será gravada para garantizar la calidad del servicio

Apreciado cliente. Los datos personales suministrados por usted, serán utilizados de conformidad con nuestras políticas de privacidad que se encuentran en nuestras páginas web:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

De conformidad con nuestras políticas ¿Autoriza usted, que LA EMRPESA le dé tratamiento a sus datos personales?

Respuesta: **Sí** (se puede continuar con la recolección de los datos)

Respuesta: No (no se puede continuar con la recolección de los datos)

12. Revocatoria de la autorización y/o supresión del dato

De acuerdo al artículo 8 del Decreto 1377, **LA EMPRESA** ha dispuesto un mecanismo gratuito y ágil a través del cual el Titular puede en todo momento, y siempre que no medie un deber legal o contractual que así lo impida, solicitar a **LA EMPRESA** la supresión de los datos personales y/o revocar la autorización que ha otorgado para el Tratamiento de los mismos, mediante la presentación de una solicitud (Ver capítulo 14 de este Manual).

Si vencido el término legal respectivo, **LA EMPRESA** no elimina de las bases de datos los datos personales del Titular que lo solicitó, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales.

13. Derechos de los titulares de los datos

La Ley 1581 de 2012, en su artículo 8, establece los siguientes derechos que le asisten al Titular en relación con sus datos personales: **a.** Conocer, actualizar, cancelar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado. **b.** Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento. **c.** Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales. **d.** Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y en las demás normas que la modifiquen, adicionen o complementen. **e.** Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. **f.** Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento. Los canales que existen en **LA EMPRESA** para el ejercicio de los derechos como Titular de los datos se encuentran previstos en el Capítulo 14 del presente Manual.

14. Procedimiento para el ejercicio de los derechos del titular de datos

Según el artículo 20 del Decreto 1377, los derechos de los Titulares establecidos en la Ley 1581, podrán ser ejercidos ante **LA EMPRESA** por las siguientes personas: **a**. Por el Titular de los datos, quien deberá acreditar ante **LA EMPRESA** su identidad en forma suficiente por los distintos medios o mecanismos que tenemos a su disposición. **b**. Por los causahabientes del Titular de los datos, quienes deberán acreditar tal calidad ante **LA EMPRESA. c.** Por el representante y/o apoderado del Titular de los datos, previa acreditación ante **LA EMPRESA** de la representación o apoderamiento. **d.** Por estipulación a favor de otro o para otro. De acuerdo con lo previsto en la ley 1581, en sus artículos 14 y 15, para el ejercicio de cualquiera de los derechos que le asisten como Titular de los datos, usted podrá utilizar ante **LA EMPRESA** cualquiera de los mecanismos que se establecen a continuación:

1. Procedimiento para Consultas: ¬ Los Titulares, sus causahabientes, sus representantes o apoderados, podrán consultar la información personal del Titular que repose en las base de datos de **LA EMPRESA**. ¬ **LA EMPRESA** como Responsable y/o Encargada del Tratamiento suministrará la información solicitada que se encuentre contenida la base de datos o la que esté vinculada con la identificación del Titular. ¬ El titular acreditará su condición mediante copia del documento pertinente y de su documento de identidad que podrá suministrar en medio físico o digital, en caso de que el titular esté representado por un tercero, deberá allegarse el respectivo poder, que deberá contener el respectivo contenido ante notario, el apoderado deberá igualmente acreditar su identidad en los términos indicados.. – La consulta se formulará a través de los canales que para dicho efecto han sido habilitados por **LA EMPRESA** y en especial a través de

comunicación escrita o electrónica, dirigida a la dependencia y persona indicada en el capítulo 18 del presente Manual.¬ La consulta será atendida por **LA EMPRESA** en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. ¬ Cuando no fuere posible para **LA EMPRESA** atender la consulta dentro de dicho término, lo informará al interesado, expresando los motivos de la demora y señalando la fecha en que atenderá su consulta, la cual en ningún caso superará los cinco (5) días hábiles siguientes al vencimiento del primer término. Se podrán consultar de forma gratuita los datos personales al menos una vez cada mes calendario, y cada vez que existan modificaciones sustanciales de las Políticas establecidas en este Manual que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **LA EMPRESA** podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos.

2. Procedimiento para Reclamos: Los Titulares, sus causahabientes, sus representantes o apoderados, que consideren que la información que se encuentra contenida en las bases de datos de **LA EMPRESA** debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante **LA EMPRESA** como Responsable y/o Encargada del Tratamiento, el cual será tramitado bajo las siguientes reglas: ¬ El reclamo se formulará mediante solicitud escrita dirigida a **LA EMPRESA**, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. ¬ Al reclamo deberá adjuntarse fotocopia del documento de identificación del Titular de los datos. ¬ El reclamo se formulará a través de los canales que para dicho efecto han sido habilitados por **LA EMPRESA**, y se dirigirá a la dependencia y a la persona indicada en el capítulo 18 del presente Manual**.**

¬ Si el reclamo resulta incompleto, **LA EMPRESA** requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. ¬ Transcurridos dos (2) meses desde la fecha del requerimiento realizado por **LA EMPRESA**, sin que el solicitante presente la información requerida, **LA EMPRESA** entenderá que se ha desistido del reclamo. ¬ En caso que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado. ¬ Una vez **LA EMPRESA** reciba el reclamo completo, incluirá en la base de datos una leyenda que indique: “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. ¬ El término máximo para atender el reclamo por parte de **LA EMPRESA** será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. ¬ Cuando no fuere posible para **LA EMPRESA** atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

3. Canales Habilitados: Los derechos de los titulares podrán ser ejercidos por las personas antes señaladas a través de los canales que han sido habilitados por **LA EMPRESA** para dicho efecto, los cuales se encuentran a su disposición de forma gratuita, así: ¬ A través de la dirección de correo electrónico: servicioalcliente@lataqueria.com.co;

Esta dirección de correo electrónico está siendo protegida contra los robots de spam. Necesita tener JavaScript habilitado para poder verlo. A través de las páginas web de LA EMPRESA:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

A través del conmutador de **LA EMPRESA**: 571-3779269 en la ciudad de Bogotá, Servicio al Cliente en el horario: De Lunes a Viernes entre de 08:00 a.m. a 12:00 m. y de 02:00 p.m. a 05:30 p.m., el cual sólo estará habilitado para el trámite de consultas, o a la siguiente dirección: Carrera 14 86ª 45, en la ciudad de Bogotá– Colombia.

15. Deberes de la Empresa como responsable y encargado del tratamiento

El artículo 17 de la ley 1581, establece los siguientes deberes para **LA EMPRESA**, como Responsable del Tratamiento de los datos de los titulares de los mismos : **a.** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; **b.** Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular; **c.** Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada **d.** Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; **e.** Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible; **f.** Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; **g.** Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento; **h.** Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley. **i.** Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular; **j.** Tramitar las consultas y reclamos formulados en los términos señalados en la ley; **k.** Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos; **l.** Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.; **m.** Informar a solicitud del Titular sobre el uso dado a sus datos; **n.** Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares. **o.** Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

El artículo 18 de la ley 1581, establece los siguientes deberes para **LA EMPRESA**, como Encargado del Tratamiento de los Datos Personales del Titular, sin perjuicio de las demás disposiciones previstas en dicha ley y en otras que rijan su actividad: **a.** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; **b.** Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; **c.** Realizar

oportunamente la actualización, rectificación o supresión de los datos; **d.** Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo; **e**. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley y en este Manual; **f.** Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares; **g.** Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la ley; **h.** Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal; **i**. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio; **j.** Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella; **k.** Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares; **l.** Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

16. Medidas de seguridad aplicadas al tratamiento de las bases de datos

Se protege la información mediante mecanismos que conservan su seguridad, confidencialidad, integridad y disponibilidad, para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento utilizando los siguientes mecanismos:

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

- Protección de acceso a los datos mediante contraseñas y roles de diferentes niveles de autoridad.

- Aseguramiento del nivel de complejidad de las contraseñas de los usuarios

17. Prohibiciones

En desarrollo de esta norma de seguridad de la información personal, se establecen las siguientes prohibiciones y sanciones como consecuencia de su incumplimiento.

- La empresa DLK S.A.S prohíbe el acceso, uso, gestión, cesión, comunicación, almacenamiento y cualquiera otro tratamiento de datos personales de carácter sensible sin autorización del titular del dato personal y/o de la empresa DLK S.A.S.

- Incurrir en esta prohibición por parte de los empleados de la empresa DLK S.A.S acarreará las sanciones a que haya lugar de conformidad con la ley.

- La empresa DLK S.A.S prohíbe la cesión, comunicación o circulación de datos personales, sin el consentimiento previo, escrito y expreso del titular del dato o sin autorización de la empresa DLK S.A.S. La cesión o comunicación de datos personales

deberá ser inscrita en el registro central de datos personales de la empresa DLK S.A.S y contar con la autorización del custodio de la base de datos.

- La empresa DLK S.A.S prohíbe el acceso, uso, cesión, comunicación, tratamiento, almacenamiento y cualquiera otro tratamiento de datos personales de carácter sensible que llegaren a ser identificados en un procedimiento de auditoría en aplicación de la norma sobre el buen uso de los recursos informáticos de la empresa y/u otras normas expedidas por la empresa DLK S.A.S para estos fines.

Los datos sensibles que llegaren a identificarse en el proceso de auditoría, serán informados al usuario del recurso informático, con el fin de que este proceda a eliminarlos; de no ser posible esta opción, la empresa DLK S.A.S procederá a eliminarlos de manera segura.

- La empresa DLK S.A.S prohíbe a los destinatarios de esta Norma cualquier tratamiento de datos personales que pueda dar lugar a alguna de las conductas descritas en la ley de delitos informáticos 1273 de 2009. Salvo que se cuente con la autorización del titular del dato y/o de la empresa DLK S.A.S, según el caso.

- La empresa DLK S.A.S prohíbe el tratamiento de datos personales de niños y adolescentes menores de edad. Todo tratamiento que se llegare a hacer respecto de los datos de los menores, se deberán asegurar los derechos prevalentes que la Constitución Política reconoce a estos, en armonía con el Código de la Infancia y la Adolescencia. En casos de tratamiento de estos datos la autorización deberá ser otorgada por los representantes legales, según el caso.

18. Designación de dependencia o persona encargada del trámite para que el titular de los datos ejerza sus derechos de peticiones, consultas y reclamos.

La responsabilidad en el adecuado tratamiento de los datos personales al interior de La empresa DLK S.A.S, está en cabeza de todos los empleados. En consecuencia, al interior de cada área que maneje los procesos de negocios que involucren tratamiento de datos personales, deberán adoptar las reglas y procedimientos para la aplicación y cumplimiento de la presente norma, dada su condición de custodios de la información personal que está contenida en los sistemas de información de LA EMPRESA.

La dependencia encargada de tramitar las consultas, quejas, reclamos y peticiones relacionados con el tratamiento y protección de los datos personales de trabajadores, clientes, proveedores, y demás titulares de los datos personales que maneja **LA EMPRESA** en sus bases de datos, será el área de Contabilidad —. La persona(s) encargada(s) será(n): —— Área de Servicio al Cliente

Sus datos de contacto son:

Teléfono: 571-6110614 en la ciudad de Bogotá

Mails: servicioalcliente@diluccatogo.com, servicioalcliente@dlksa.net

Dirección: Carrera 14 86ª 45, Bogotá – Colombia

Página web:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

19. Modificación de la Política de tratamiento

La empresa DLK S.A.S informarán a los titulares de Datos en caso de presentarse cambios sustanciales en el contenido de este Manual de Políticas de Tratamiento de Datos Personales, referidos a la identificación del Responsable y/o Encargado y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización que los titulares han otorgado a la empresa DLK S.A.S Asimismo se le comunicará a los titulares sobre dichos cambios antes o a más tardar al momento de la implementación de las nuevas políticas.

Además, cuando el cambio se refiera a la finalidad del Tratamiento de los datos personales, **LA EMPRESA** obtendrá una nueva autorización de parte de los titulares. Para ello hemos dispuesto en el sitio web de la empresa DLK S.A.S nuestros canales web:

- http://www.diluccatogo.com

- http://www.dlkrestaurantes.com

, a través de los cuales se le informará sobre el cambio y se pondrá a su disposición la última versión de este manual o los mecanismos habilitados por **LA EMPRESA** para obtener una copia de la misma.

20. Entrada en vigencia de la Política de Tratamiento

La presente Política de Tratamiento de Datos Personales fue creada el día diciembre (01) del mes de diciembre del año dos mil dieciséis (2016) y empieza a regir a partir del primero (01) de marzo del año dos mil diecisiete (2017).

Atentamente,

CAMILO LLERAS MEJIA
DLK S.A.S
NIT. 800.095.036-4

POLÍTICA SEGURIDAD DE LA INFORMACIÓN

MANUAL INTERNO DE POLÍTICAS Y DE PROCEDIMIENTOS PARA LA SEGURIDAD DE LA INFORMACION -TIC

- **DLK S.A.S.**

DICIEMBRE DE 2016

Contenido

1. OBJETIVO

Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental.

2. ALCANCE

Esta Política es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de la organización.

3. LÍNEA BASE DE LA POLÍTICA

3.1 RESPONSABILIDAD

Es responsabilidad de la Dirección de Tecnología hacer uso de la Política de Seguridad de la Información, como parte de sus herramientas de gobierno y de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

3.2 CUMPLIMIENTO

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

3.3 EXCEPCIONES

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por la Dirección de Tecnología, la cual puede requerir autorización de la Gerencia de General. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

3.4 ADMINISTRACIÓN DE LAS POLÍTICAS

Las modificaciones o adiciones de la Política de Seguridad de la Información serán propuestas por la Gerencia de la compañía, la Subgerencia, por medio de la Gerencia General y serán aprobadas por la Junta Directiva. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

4. DESCRIPCIÓN DE LAS POLÍTICAS Y ESTÁNDARES

Generalidades

La información es un activo que la compañía considera esencial para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad. A través de esta Política se difunden los objetivos de seguridad de la información de la compañía, que se consiguen a través de la aplicación de controles de seguridad, para gestionar un nivel de riesgo aceptable. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos de negocio y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en DLK S.A.S.

4.1 ORGANIZACIÓN DE SEGURIDAD

Política de la organización de seguridad

La Dirección de Tecnología es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en DLK S.A.S y reportará a la Gerencia General, dicho comité debe contar con la presencia de personal clave y claramente definido, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

Estándares de la Política de la organización de seguridad

• **Responsabilidades para la seguridad de la información**.
DLK S.A.S es el propietario de la información. Su tenencia y manejo es delegada a los gerentes de la compañía, quienes son responsables de la custodia de la información que las administradores generan, considerando su propósito y uso. Por ello los gerentes deben ser conscientes de los riesgos a la que está expuesta la información a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para disminuirlos.

• **Contacto con autoridades y grupos de interés.**
DLK S.A.S debe mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.

Revisión independiente en seguridad de la información. Auditoría Interna debe implementar y ejecutar un plan interno de auditoría de seguridad de la información. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por la Dirección de tecnología y Seguridad de la Información.

Seguridad en los Accesos por Terceros. La Dirección de Tecnología debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de DLK S.A.S. Cada Administrador debe verificar la implementación de acuerdos, monitorear el

cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

4.2 CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

Política para la clasificación y control de activos de información

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada como secreta, restringida o general.

La información secreta y restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

Estándares de la Política de clasificación y control de activos de información

• **Responsabilidad sobre los activos**.
DLK S.A.S pone al servicio de los colaboradores el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

• **Metodología de clasificación de activos.**
Para asegurar que los activos de información reciben el nivel de protección adecuado, la Dirección de Tecnología es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.

4.3 USO ACEPTABLE DE LOS ACTIVOS Y RECURSOS

Política de Uso Aceptable de los Activos y Recursos de información

Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de DLK S.A.S, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados.

Estándares para el uso aceptable de los activos de información

• **Uso de los sistemas y equipos de cómputo**.
La organización tiene regla de renuncia (disclaimer) que debe utilizarse al inicio de sesión en los equipos de cómputo: “Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la empresa y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema

dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política."

- **Correo electrónico.**

La organización, como muestra del respeto por los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la compañía; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado. Las comunicaciones por correo electrónico entre la empresa y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, ni para transmitir cualquier otro tipo de información del negocio.

A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. La Direccion de Gestión Humana y Administrativa es responsable de informar a la Dirección de Tecnología, las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de colaboradores para la suspensión de este servicio.

Esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la Compañía, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de servicios.

La capacidad máxima para almacenamiento de correo electrónico está definida por la Dirección de Tecnología y depende del tipo de usuario. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad. De igual manera, en caso de necesidad (por razones del negocio o técnicas), las capacidades máximas de los buzones podrán ser modificadas unilateralmente por parte de la compañía.

El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.

La organización tiene regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes.

Para evitar reclamaciones legales todos los usuarios de correo de la empresa tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información.

El disclaimer aprobado es:

La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente y bórrela puesto que su uso no autorizado acarreará las sanciones y medidas legales a que haya lugar. La empresa no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información.

"The information contained in this message and its attachments is strictly confidential. If you received this communication in error, please immediately notify the sender of the situation by replying it to sender email address and delete this message as its unauthorized use shall derive in applicable penalties and legal actions.. The Company is not liable for the presence of any virus or malware in this message or its attachments that cause or may cause damage to your equipment, software or that affects your information."

El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la organización, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
- El colaborador titular de correo o cuenta asignada por la organización, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo o de las investigaciones que tenga asignadas; las únicas áreas autorizadas para el envío de correos masivos son la Áreas de Mercadeo y Administrativas de Asuntos Corporativos (a través de la gerencia Operativa y Administrativa) y la Dirección de Tecnología.

Otras necesidades de comunicación masiva deben ser aprobadas por las direcciones de Tecnología y Comunicaciones:

- El uso del correo electrónico propiedad de la compañía deberá ser usado solamente para fines propios a la organización. En su uso el colaborador actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.
- La compañía se abstiene de enviar o recibir los mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.
- Los colaboradores de la compañía se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes *spam* (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), *hoax* (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.
- Evitar el envío desde su buzón de elementos (textos, *software*, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de *software* que requiera licencia, claves ilegales de *software*, programas para romper licencias (*crackers*), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
- Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencias de espacio disponible. Estas advertencias se realizan varias veces, por lo que debe estar atento e informar a la mesa de servicios informáticos, cuando requiera la depuración del mismo.
- Utilizar la cuenta de correo electrónico corporativa para fines laborales, de investigación y los estrictamente relacionados con las actividades propias de su trabajo. Los colaboradores

deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la empresa.

- El colaborador debe depurar mensualmente el contenido del buzón de entrada en el servidor para evitar que los mensajes permanezcan en él un tiempo excesivo que conduzca a la congestión o al bloqueo del mismo.
- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa.
- Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.
- Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando.
- En lo posible, es necesario evitar usar letras mayúsculas, especialmente en el campo de "Asunto:", al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, ¡, !, ¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado o *spam*, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.
- Si utiliza el servicio de correo a través del sitio web de la empresa, se recomienda que no deje mensajes almacenados por mucho tiempo en el servidor de correo. Tenga presente descargarlos con frecuencia, preferiblemente a diario. Tenga en cuenta que el tamaño de su buzón de correo es limitado; una vez superado este tope, el sistema no le procesará más correos. Elimine mensajes si lo necesita y vacíe la papelera siempre que sea posible.

- **Navegación en Internet**.

El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el colaborador para realizar las funciones establecidas para su cargo, por lo cual la compañía definió los siguientes parámetros para su uso:

- El colaborador debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía *web* o medios magnéticos.
- La descarga de música y videos no es una práctica permitida.
- Evitar el uso de servicios descarga de archivos como: *KaZaA, Emule, LimeWire, Morpheus, GNUtella* o similares.
- Las salas de video-conferencia de la organización deben ser de uso exclusivo para asuntos relacionados con la empresa. Cualquier excepción a esta política debe ser autorizada por la Dirección de Tecnología.
- Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet (*proxy*).
- El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- Los colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona.

- Abstenerse de coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley estatal, local, nacional o internacional; incluyendo, pero no limitado, las leyes y regulaciones de control y exportación de Colombia y de los decretos sobre fraudes de computación.
- Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social, marital, ocupacional, financiera, y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la compañía.
- Los colaboradores se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.
- Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas se constituyen como violaciones a esta Política.
- No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.
- Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta Política.

- **Uso de herramientas que comprometen la seguridad**.

Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la Dirección de Tecnología, cualquiera de los siguientes actos:

o Acceder el sistema o red.
o Monitorear datos o tráfico.
o Sondear, copiar, probar *firewalls* o herramientas de *hacking*.
o Atentar contra la vulnerabilidad del sistema o redes.
o Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

- **Recursos compartidos**.

El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

- Se debe evitar el uso de carpetas compartidas en equipos de escritorio.
- Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través de la Mesa de Servicios.
- El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
- Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
- Si se trata de información confidencial o crítica para la empresa, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
- El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.

➢ No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

• **Sitios Web para compartir documentos**.
El dueño del sitio será el responsable de la seguridad del mismo y del acceso a la información que se encuentra alojada.
o El dueño del sitio será el responsable de otorgar los permisos requeridos.
o El dueño del sitio definirá un delegado que tengan control total sobre el sitio, a manera de contingencia, para la asignación de los permisos requeridos en su ausencia.

• **Computación en nube**.
Ninguna información de DLK S.A.S podrá utilizar tecnologías de computación en nube si no está previamente autorizado por la Dirección de Tecnología.

• **Uso equipos portátiles y dispositivos móviles.**
Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:
o El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.
o El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
o Uso de aplicación de antivirus.
o Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

• **Acceso de equipos distintos a los asignados.**
o Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.
o No dejar claves en ningún sistema de almacenamiento de información web.
o Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
o Cerrado de sesión de escritorio virtual cuando no esté en uso.

La Dirección de Tecnología debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.

La utilización de los servicios móviles conectados a las redes, debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

4.4 TRATAMIENTO Y GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

La Dirección de Tecnología, es responsable de analizar los riesgos en seguridad de la información, con base en los objetivos de negocio y de acuerdo con la Política de Gestión de Riesgos y con aprobación del Comité de Seguridad de la Información.

Los administradores son responsables de priorizar y realizar el tratamiento de los riesgos en seguridad de la información de acuerdo con el apetito de riesgo de la empresa.

Estándares de la Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables.

Los posibles tratamientos a los riesgos identificados incluyen:
- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

4.5 SEGURIDAD DEL PERSONAL

Política de Responsabilidad del Personal

La Direccion de Gestión Humana debe notificar a la Dirección de Tecnología todas las novedades del personal directo e indirecto tales como ingresos, traslados, delegaciones, retiros y vacaciones.

Estándares de la Política de Seguridad del Personal

- **Seguridad previa a la contratación del personal**.

Para toda persona que ingrese a la compañía, la Vicepresidencia de Gestión Humana y Administrativa debe asegurar las responsabilidades sobre seguridad de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación.

• **Seguridad durante el contrato**.
La Direccion de Gestión Humana y Administrativa debe desarrollar un programa efectivo y continuo de concientización de protección de la información para todo el personal. También se requiere de capacitación específica en administración de riesgos tecnológicos para aquellos individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador.

Es responsabilidad y deber de cada colaborador de DLK S.A.S asistir a los cursos de concientización en seguridad de la información que la empresa programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la empresa.

• **Finalización o cambio de puesto**.
La Direccion de Gestión Humana y Administrativa debe asegurar que todos los colaboradores, consultores, contratistas, terceras partes, que salgan de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que DLK S.A.S lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato.

La Direccion de Gestión Humana y Administrativa se asegurará que la salida o movilidad de los colaboradores, contratistas o terceros sea gestionada hasta la completa devolución de todos los activos y retirada de los derechos de acceso.

4.6 SEGURIDAD FÍSICA Y DEL ENTORNO

Política de Seguridad Física y del Entorno

El centro de procesamiento de datos y cuarto de equipos de TIC, deben de estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.

Estándares de la Política de Seguridad Física y del Entorno

• **Controles de acceso físico.**
El acceso a áreas TIC restringidas sólo se debe permitir para:
- Desarrollo de operaciones tecnológicas.
- Tareas de aseo (monitoreado por personal de la Dirección de Tecnología).
- Pruebas de equipos.
- Almacenamiento de equipos.
- Implementación o mantenimiento de los controles ambientales.

• **Escritorio limpio.**

Política Seguridad de la información

La implementación de una directriz de escritorio limpio permitirá reducir el riesgo de acceso no autorizado o daño a medios y documentos.

Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los colaboradores, consultores, contratistas, terceras partes, deben bloquear la sesión al alejarse de su computador.

- **Seguridad de los equipos.**

Para prevenir la pérdida de información daño o el compromiso de los activos de información y la interrupción de las actividades de DLK S.A.S, los equipos deben estar conectados a la toma regulada destinada para tal fin.

- **Retiro de equipos.**

Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo.

4.7 CONTROL DE ACCESO A LA INFORMACIÓN

Política de Control de Acceso a la Información

La Dirección de Tecnología, conforme la clasificación de activos de información, debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento.

El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.

Estándares de Política de Control de Acceso a la Información

- **Gestión de acceso a usuarios.**

La Dirección de Tecnología establecerá procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por la Gerencia responsable del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados.

- **Registro de usuarios.**

Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizará para el seguimiento de las actividades de responsabilidad individual o jurídica. Las actividades habituales de usuario no deben ser desempeñadas a través de cuentas privilegiadas.

En circunstancias excepcionales, por beneficio de la compañía, se podrá usar un identificador compartido, para un grupo de usuarios con trabajo específico; este debe ser autorizado y debidamente aprobado por la respectiva Dirección de Gestión de Tecnología.

El usuario debe tener autorización de la respectiva vicepresidencia para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la empresa y conserven una adecuada segregación de funciones.

Adicionalmente, deben tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

• **Responsabilidades del usuario.**
Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, La Dirección de Tecnología implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario implementar un procedimiento de revisión periódica de los permisos de acceso de los usuarios.

Los colaboradores, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este. Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

• **Control de acceso a la red.**
Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

• **Control de acceso a las aplicaciones.**
El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

Las sesiones inactivas deben cerrarse después de un período de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.

Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o software.

La Dirección de Tecnología debe integrar las aplicaciones con el Directorio Activo.

4.8 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Política de Gestión de incidentes de Seguridad de la Información

Todos los colaboradores, consultores, contratistas, terceras partes, deben anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios a través de la mesa de servicios.

Estándares de la Política de Gestión de Incidentes de Seguridad de la Información

• **Notificación de eventos y debilidades de seguridad de la información.**
La Dirección de Tecnología debe asegurarse de que los eventos y los puntos débiles de seguridad de la información asociados con los sistemas de información, se comunican de forma que sea posible emprender acciones correctivas.

Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, que determine la respuesta que debe darse cuando se recibe un informe de un evento de seguridad de la información.

• **Gestión de incidentes de seguridad de la información.**
Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, el grupo de resolución de problemas se encargará de analizar la causa y evaluar conforme al proceso de gestión de problemas.

Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro que se destruyan de forma intencional o accidental de las pruebas necesarias antes de tomar conciencia de la gravedad del incidente. Se debe hacer uso de los servicios jurídicos de DLK S.A.S y/o de la Policía en las primeras fases de cualquier acción legal que se esté considerando, así como asesorarse de las pruebas necesarias.

Cuando una acción contra una persona u organización, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas legales vigentes. A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

4.9 GESTIÓN DE SEGURIDAD PARA TELECOMUNICACIONES E INFRAESTRUCTURA DE TIC

Política de Gestión de Telecomunicaciones e Infraestructura de TIC

La Dirección de Tecnología debe proveer el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación, a través de una Gestión de Telecomunicaciones e Infraestructura de TIC efectiva y eficiente.

Estándares de la Política de la Política de Gestión de Telecomunicaciones e Infraestructura de TIC

• **Procedimientos y responsabilidades de operación.**
La Dirección de Tecnología debe definir y documentar claramente las responsabilidades para el manejo y operación de instalaciones de computadores y redes, apoyadas por instrucciones operacionales apropiadas incluyendo procedimientos de respuesta en caso de incidentes.

La Dirección de Tecnología debe definir controles que garanticen la apropiada operación tecnológica. Estos controles deben incluir como mínimo los siguientes procedimientos:

- Copias de seguridad.
- Verificación de cintas.
- Recuperación de datos y reversión de cambios.
- Administración de sistemas de antivirus.
- Administración de usuarios y contraseñas.
- Administración de acceso a los recursos.
- Administración de acceso remoto.
- Medición de desempeño.
- Capacidad y disponibilidad de los recursos de TI.
- Gestión de pistas de auditoria y sistemas de registro de información.
- Aseguramiento de plataformas.

- **Gestión del Cambio.**

La Dirección de Tecnología debe implementar los controles necesarios que permitan garantizar la segregación de funciones y un adecuado seguimiento a los cambios efectuados a los activos críticos de TI. La documentación debe incluir, entre otros:

o Persona que solicita el cambio.
o Responsable de autorización.
o Descripción del cambio.
o Justificación del cambio para el negocio.
o Lista de chequeo para evaluación de riesgos, sistemas y/o dispositivos comprometidos.
o Nivel de impacto.
o Pruebas, aprobación revisiones de post-implementación.
o Capacitación, cuando sea necesario.

- **Segregación de funciones.**

Las tareas y responsabilidades propias de gestión de tecnología, se deben segregar para reducir e impedir las oportunidades de acceso no autorizado a la red y cualquier modificación o mal uso de los activos de los sistemas de información. Se prestará especial cuidado que una persona no pueda por si misma acceder, modificar o utilizar los activos, sin previa autorización.

- **Separación de Ambientes.**

Cuando aplique los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados, prevenir fallos e implementar controles.

- **Planificación y Aceptación.**

Se deben definir los requisitos de capacidad futura, con el fin de reducir el riesgo a una sobrecarga del sistema. Los requisitos operativos de sistemas nuevos se deben establecer, documentar y probar antes de su aceptación. Los requisitos de restitución para los servicios apoyados por diferentes aplicaciones se deben coordinar y revisar frecuentemente. Los administradores de TI deben estar alerta a los riesgos asociados a estas tecnologías, así mismo considerar la toma de medidas especiales para su prevención o detección.

- **Protección contra el código malicioso.**

La Dirección de Tecnología debe implementar controles de detección, prevención y recuperación para la protección frente al código malicioso. Los usuarios deben ser conscientes de los peligros de los códigos maliciosos. En DLK S.A.S no está permitido el uso de *software* no licenciado y su instalación en cualquiera de los equipos de la compañía.

• **Copias de seguridad.**
Se deben hacer copias de respaldo de la información y del *software*. Para garantizar la integridad y disponibilidad, se debe hacer su comprobación regular de los mecanismos y la información en conformidad con la política de respaldo acordada, conservando los niveles de confidencialidad requeridos. La Dirección de Gestión de Tecnología debe almacenar las copias de seguridad por fuera de las instalaciones de DLK S.A.S con el fin de garantizar su recuperación en caso de un evento mayor en la sede principal.

• **Gestión de seguridad en las redes.**
Se le debe dar atención especial al manejo de la seguridad en redes, la cual puede extenderse más allá de los límites físicos de DLK S.A.S. Procedimientos y medidas especiales se requieren para proteger el paso de información sensible a redes de dominio público. La Dirección de Tecnología debe garantizar que los proveedores de servicios de red implementan medidas en cumplimiento con las características de seguridad, acuerdos de niveles de servicio y requisitos de gestión.

Se deben establecer controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas, igualmente se debe garantizar la disponibilidad de los servicios de red y computadores conectados.

• **Servicios de Comercio Electrónico.**
Se debe realizar una evaluación para identificar el riesgo asociado con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles.

Se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

• **Monitoreo de uso del sistema.**
El nivel de monitoreo necesario para los servicios se determinará mediante una evaluación de riesgos. DLK S.A.S cumplirá los requisitos legales que se apliquen en sus actividades de monitoreo.

Se deben registrar las actividades tanto del operador como del administrador del sistema. Las actividades a monitorear incluyen: operaciones privilegiadas, acceso no autorizado y alertas o fallas del sistema, entre otras.

• **Registros de Auditoría.**
Se deben elaborar y mantener durante un período acordado, los registros de auditoría de las actividades de usuario, de operación y administración del sistema.

• **Protección de la información de registro.**
Los servicios y la información de la actividad de registro se deben proteger contra el acceso o manipulación no autorizados.

• **Tratamiento de medios con información.**
Se deben controlar los medios y proteger para prevenir la revelación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades del negocio.

La Dirección de Tecnología debe implementar los controles que permitan garantizar que la eliminación de cualquier dispositivo o componente tecnológico que contenga información sensible, sean destruidos físicamente, o bien que la información sea destruida, borrada o

sobrescrita, mediante técnicas que no hagan posible la recuperación de la información original, en lugar de utilizar un borrado normal o formateado.

• **Sincronización de relojes.**
Los relojes de los sistemas dentro de DLK S.A.S deben estar sincronizados con un tiempo acordado. Debe establecerse según una norma aceptada, por Ej. PST o un tiempo normalizado local.

4.10 GESTIÓN DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Política de Adquisición, Desarrollo y Mantenimiento de sistemas

La Dirección de Tecnología debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento.

Estándares de la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

• **Requerimientos de seguridad de los sistemas.**
La Dirección de Tecnología debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, consideren la administración de los riesgos de seguridad. Todos los requerimientos de seguridad se deben identificar durante la etapa de requerimientos, al igual que justificar, acordar y documentarse, como parte de todo el proyecto del sistema de información.

• **Seguridad de las aplicaciones del sistema.**
Se deben desarrollar estándares que indiquen cómo se deben asegurar los diferentes sistemas, aplicaciones y desarrollos, para minimizar la aparición de errores, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones.

Se deben diseñar controles adecuados en las aplicaciones, para garantizar un correcto procesamiento. Se debe incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes.

Las aplicaciones que se desarrollen en DLK S.A.S deben cumplir unos requerimientos mínimos de seguridad, conforme a las buenas prácticas en seguridad de la información y a esta política de seguridad. El diseño y operación de los sistemas debe obedecer a estándares de seguridad comúnmente aceptados y la normatividad vigente.

• **Seguridad de los sistemas de archivos.**
Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del *software* aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.

• **Seguridad de los procesos de desarrollo y soporte.**
Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control no estén

comprometidos; igualmente deben cerciorarse de que los programadores de apoyo posean acceso sólo a las partes en el sistema necesarias para desarrollar su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

4.11 CUMPLIMIENTO Y NORMATIVIDAD LEGAL

Política para el Cumplimiento y Normatividad Legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

Estándares de la Política para el Cumplimiento y Normatividad Legal

- **Cumplimiento legal.**

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información de DLK S.A.S, deben definirse previamente y documentarse de acuerdo con la metodología empleada por la empresa. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. El área jurídica de DLK S.A.S asesorará al Comité de Seguridad en dichos aspectos legales específicos.

- **Propiedad intelectual.**

Se protegerá adecuadamente la propiedad intelectual de DLK S.A.S, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

- **Protección de datos.**

Los estándares de seguridad son de obligatorio cumplimiento para los colaboradores con acceso a los datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:

- Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.
- Funciones y obligaciones del personal con acceso a las bases de datos.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante los incidentes.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente.
- Medidas a adoptar cuando un soporte o documento va ha ser transportado, desechado o reutilizado.

El procedimiento se mantendrá actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

- **Cumplimiento de políticas y normas de seguridad.**

Los directivos de la compañía se deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluaran y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión con auditoria.

- **Cumplimiento técnico.**

Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deben realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad de la información, las vulnerabilidades y su grado de exposición al riesgo.

5. DOCUMENTACIÓN RELACIONADA

- Código de Buen Gobierno Corporativo.
- Sistema de Gestión de la Calidad y Política Ambiental de la organización.
- Política de Gestión Humana.
- Política de Gestión de Riesgos
- Política de tecnología de información y comunicación.

6. DEFINICIONES

Para los propósitos de este documento, se definen los siguientes conceptos:

- **Activo:** cualquier cosa que tenga valor para la empresa.
- **Amenaza**: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Comité de Seguridad de la Información:** el Comité de Seguridad de la Información debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de la información de DLK S.A.S, aplicando los principios de confidencialidad, integridad y disponibilidad de la misma y de los recursos informáticos o de otra índole que la soportan, acorde con la planeación estratégica de la empresa.
- **Desastre o contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Estándares de seguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad

disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de *hardware, software* o infraestructura.

- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.
- **Impacto:** la consecuencia que al interior de la empresa se produce al materializarse una amenaza.
- **Organización de seguridad:** es una función que busca definir y establecer un balance entre las responsabilidades y los requerimientos de los roles asociados con la administración de seguridad de la información.
- **Políticas:** toda intención y directriz expresada formalmente por la dirección**.**
- **Procesos:** se define un proceso de negocio como cada conjunto de actividades que reciben una o más entradas para crear un producto de valor para el cliente o para la propia empresa (concepto de cliente interno de calidad). Típicamente una actividad empresarial cuenta con múltiples procesos de negocio que sirven para el desarrollo de la actividad en sí misma.
- **Procedimientos:** los procedimientos son los pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos.
- **Riesgo:** combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*accountability*), no repudio y fiabilidad.
- **TI:** se refiere a tecnologías de la información
- **TIC:** se refiere a tecnologías de la información y comunicaciones
- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

7. CONTROL DE CAMBIOS

VERSION	FECHA	JUSTIFICACION DE LA VERSION
1	01/12/2016	Creación de la Política TIC