NIT. 900065780-0

POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

TRANSARMENIA CARGA S.A. DE FAMILIA, identificada con NIT. 900.065.780-0, con domicilio principal en la ciudad de Armenia – Quindío, en la carrera 19 #45-19, con números de contacto (6)7341660, celular 3217359150; correo electrónico transarmeniacarga@transarmenia.com, protecciondedatos@transarmenia.com, con página web www.transarmenia.com, como empresa responsable del tratamiento de datos personales, y de acuerdo a lo estipulado en la Ley 1581 de 2012 y el Decreto 1377 de 2013, expide las siguientes Políticas para el Tratamiento de Datos Personales:

A- NORMATIVIDAD LEGAL Y ÁMBITO DE APLICACIÓN: Las políticas aquí plasmadas de Tratamiento de Datos Personales, están sujetas a la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto Único Reglamentario 1074 de 2015 y las demás disposiciones acordes al fin de las mismas, que serán aplicadas por TRANSARMENIA CARGA S.A. DE FAMILIA, sobre la recolección, almacenamiento, uso, circulación, supresión de todas las acciones que conformen el tratamiento de datos personales.

B- DEFINICIONES: Para efectos de las presentes políticas de tratamiento de datos personales, y de acuerdo a la normatividad que les rigen, se tendrán presentes las siguientes definiciones, que lleven a una mejor interpretación y entendimiento de las políticas:

- ✓ **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- ✓ **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el responsable, que se pone a disposición del titular, para el tratamiento de sus datos personales. En el Aviso de Privacidad se comunica al titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y la finalidad del tratamiento que se pretende dar a los datos personales.
- ✓ **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- ✓ **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- ✓ **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.
- ✓ **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.
- ✓ **Titular:** Persona natural, cuyos datos personales sean objeto de Tratamiento.
- ✓ **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión de los mismos.

C- FINALIDAD PARA LA CUAL SE HACE LA RECOLECCIÓN DE DATOS PERSONALES Y TRATAMIENTO DE LOS MISMOS: TRANSARMENIA CARGA S.A. DE FAMILIA, podrá hacer uso de los datos personales

para: Operación de mensajería – paqueteo y carga; recogida y entrega de mercancía; verificación de información para clientes crédito; verificación y registro de información para elaboración de manifiestos de carga; diligenciamiento de guías de operación de mensajería y paqueteo; envío de información solicitada por el mismo cliente con su cuenta de cobro; gestión de recuperación de cartera; verificación de referencias y antecedentes de candidatos a vacantes; actualización de información de asociados de negocios (clientes/proveedores); actualización de información de funcionarios.

D- DERECHOS DE LOS TITULARES DE DATOS PERSONALES OBJETO DE TRATAMIENTO, POR PARTE DE TRANSARMENIA CARGA S.A.: Los titulares de datos personales por sí, o por intermedio de su representante y/o apoderado, podrán ejercer los siguientes derechos, de acuerdo a lo estipulado en la Ley, y serán de cumplimiento del Responsable del Tratamiento:

- ✓ Conocer, actualizar y rectificar los Datos Personales frente a los responsables del Tratamiento o encargados del Tratamiento.
- ✓ Solicitar prueba de la autorización otorgada al Responsable del Tratamiento, salvo cuando expresamente esté exceptuado por la Ley, como requisito para el Tratamiento.
- ✓ Ser informado, por el Responsable del Tratamiento o el encargado del Tratamiento, cuando así lo solicite, sobre el uso que le ha dado a los Datos Personales.
- ✓ Presentar ante la autoridad competente quejas por infracciones a la normativa de protección de datos.
- ✓ 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, previa verificación por parte de la autoridad competente.
- ✓ Acceder gratuitamente a los Datos Personales que hayan sido objeto de Tratamiento.
- ✓ Los demás derechos consagrados en las Políticas de Tratamiento de Datos Personales de TRANSARMENIA CARGA S.A.

E- PRINCIPIOS: Los principios bajo los cuales se rigen las Políticas de Tratamiento de Datos Personales de TRANSARMENIA CARGA S.A., son:

- ✓ **Principio de Legalidad:** El Tratamiento de datos personales, es una actividad regulada que debe sujetarse a lo establecido en la Ley y las demás normas que lo sustenten.
- ✓ **Principio de Finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución Política y la Ley, la cual debe ser informada al Titular.
- ✓ **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 Libertad:** El Tratamiento sólo puede ejercerse con el consentimiento previo, expreso, e informado del Titular. Los datos personales no podrán ser obtenidos sin previa autorización, o en ausencia del mandato legal o judicial que releve el consentimiento.
- ✓ **Principio de Transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable de tratamiento o el 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 caso, 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.

F- ÁREA RESPONSABLE Y PROCEDIMIENTO ESTIPULADO PARA EL TRATAMIENTO Y GARANTÍA DE LOS DERECHOS A LOS TITULARES DE LOS DATOS PERSONALES: La Subgerencia de TRANSARMENIA CARGA S.A., será la responsable de atender las peticiones, quejas y reclamos que tengan lugar por parte del titular de los datos, de acuerdo a los derechos a los que es acreedor, mencionados en el literal d de las presentes políticas. Para tal fin, el titular de los datos personales, o su representante, podrá hacer su solicitud física en la carrera 19 #45-19 de Armenia - Quindío, o a través del correo electrónico protecciondedatos@transarmenia.com; o comunicándose con nuestras líneas (6)7341660, celular 3217359150, de lunes a viernes de 8:00 a.m., a 12:00 m; de 2:00 p.m., a 6:00 p.m., y los sábados de 8:00 a.m., a 12.00 m. Reiteramos que la petición, queja o reclamo, deberá contener la información estimada en el FORMATO DE RECLAMACIONES PARA DATOS PERSONALES, que puede solicitar a través del correo electrónico mencionado en las políticas o a través de la página www.transarmenia.com, y se cumplirán los términos allí establecidos.

G- VIGENCIA DE LAS POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES: Las políticas de tratamiento de datos personales, fueron creadas el 1 de junio de 2017, con entrada en vigencia a partir de la misma fecha. En caso de presentarse cambios o ajustes a las mismas, éstas serán publicadas a través de la página web www.transarmenia.com

H- AUTORIZACIÓN DEL TITULAR DEL USO DE SUS DATOS PERSONALES: Al momento de efectuar la utilización de los datos personales del titulares, o previo a ello, TRANSARMENIA CARGA S.A., deberá solicitar la autorización del titular, mediante documento escrito, medios sistematizados o de manera verbal, para llevar a cabo la recolección y tratamiento de los mismos. De igual manera, deberá informar el fin para el cual requiere dichos datos y el tiempo por el cual serán utilizados, teniendo en cuenta los usos estimados en la normatividad vigente.

I- AVISO DE PRIVACIDAD: En caso tal, de que TRANSARMENIA CARGA S.A., no tenga al alcance la disposición de las políticas de tratamiento de datos personales, para el titular, será publicado el aviso de privacidad permanentemente de manera física en las instalaciones de la misma, y a través de medios virtuales, para que sea de consulta del titular y de la entidad competente de vigilancia y control.

J- POLÍTICAS DE SEGURIDAD PARA EL PERSONAL: En cuanto a la vinculación de personal, TRANSARMENIA CARGA S.A., realizará las verificaciones necesarias establecidas en el proceso de Talento Humano BASC, con el fin de confirmar la veracidad de la información suministrada por el candidato de la vacante del momento, posterior a la autorización del titular de los datos, dándole a conocer que es el protocolo del proceso.

En caso de ser seleccionado, el nuevo empleado, deberá firmar una CLAÚSULA DE CONFIDENCIALIDAD, y una CLAÚSULA DE RESPONSABILIDAD de la información a la cual tenga acceso para el desarrollo de sus funciones, quedando igualmente estipulado en el manual de funciones.

De igual manera, TRANSARMENIA CARGA S.A., capacitará y sensibilizará al personal que ingresa como el ya existente, en la responsabilidad con la seguridad de la información, para evitar posibles riesgos de pérdida de la información.

Así mismo, TRANSARMENIA CARGA S.A., aplicará el proceso disciplinario sancionatorio, descrito en el reglamento interno de trabajo, correspondiente a la indebida utilización de datos personales, una vez sean comprobadas las violaciones o incumplimientos de las políticas tratamiento de datos personas, asumiendo igualmente la responsabilidad civil y penal, si el caso llega a esta instancia.

En cuanto a la desvinculación del personal, se tendrá por estimado que una vez finalice la relación laboral, la información que se ha recopilado durante la duración de su contrato de trabajo, será almacenada en el archivo inactivo de la empresa, asegurando la adecuada custodia.

Al finalizar la ejecución del contrato por prestación de servicios por parte de terceros, la información que se ha recopilado durante el tiempo del contrato, será almacenada en el archivo según las políticas contables establecidas, asegurando su adecuada custodia.

Por último, cuando un aspirante a vacante, presente su hoja de vida, ésta deberá ser entregada o enviada a Talento Humano, y se recibirá conjuntamente con la firma de autorización de uso de los datos personales para su verificación y proceso establecido para el caso, en caso de no ser seleccionado, se le informará al aspirante que tiene un término de cinco (5) días hábiles para reclamar nuevamente su hoja de vida, a partir de recibida la comunicación que no fue seleccionado, si pasados estos cinco (5) días, no se acerca a reclamarla, se le llamará nuevamente, dejando evidencia de la misma en un registro con soporte de fecha, hora, objeto de llamada, respuesta y observaciones, dando un término de treinta (30) hábiles para que se acerque a reclamar su hoja de vida, tiempo en el cual, ésta estará protegida y archivada, si no acude al segundo llamado, dará por entendido que dicha hoja de vida puede ser suprimida, protegiendo que sus datos no queden expuestos en la empresa. La presente información, será informada y autorizada mediante formato, al momento de entregar la hoja de vida.

Si la hoja de vida es recibida por correo electrónico, una vez se reciba se enviará por el mismo medio el formato de autorización de tratamiento de datos personales, y sólo se tomará como aceptada la hoja de vida para iniciar proceso de pre selección, una vez se reciba por el mismo medio la autorización, si pasados cinco (5) días, no se recibe dicha autorización, se le reenviará la hoja de vida, dejando como soporte el correo de envío con la novedad de por qué no fue tenida en cuenta.

K- <u>POLÍTICAS RELACIONADAS CON EL MANEJO DE LA INFORMACIÓN PERSONAL:</u> TRANSARMENIA CARGA S.A., velará por la protección de la privacidad de la información personal de sus clientes finales, proveedores, contratistas, visitantes, empleados, ex empleados y demás titulares de información, estableciendo los controles necesarios para preservar los datos que le reciban de ellos, propiciando que dicha información sea utilizada únicamente para las funciones propias de la necesidad requerida por el Responsable del Tratamiento de los datos personales, y no sea publicada, revelada o entregada a terceras partes sin autorización, salvo por las disposiciones legales requeridas.

Con el fin de establecer los debidos procedimientos de responsabilidades y autorizaciones en el tratamiento de la información personal, TRANSARMENIA CARGA S.A., identificará las responsabilidades y autorizaciones para los cargos involucrados en el manejo de la información personal de sus clientes finales, proveedores, contratistas. Visitantes, empleados, ex empleados y demás titulares de datos, para posteriormente asignar la responsabilidad del cuidado de dichos datos, mediante ACTA DE ASIGNACIÓN DE RESPONSABILIDADES, y estipulado en el manual de funciones.

L- POLÍTICA DE ÉTICA EN MANEJO DE DATOS PERSONALES:

Compromiso de los directivos y ejecutivos con la ética.

- Los altos directivos y ejecutivos dentro de TRANSARMENIA CARGA S.A. deben dar un buen ejemplo. En cualquier práctica empresarial, la honestidad y la integridad deben ser la máxima prioridad para el personal. Los directivos y ejecutivos deben tener una política de puertas abiertas y agradecer sugerencias e inquietudes de los colaboradores. Esto permitirá que los colaboradores se sientan cómodos discutiendo cualquier problema y alertarán a los directivos y ejecutivos de las preocupaciones dentro de la fuerza de trabajo.
- Los directivos y ejecutivos dentro de TRANSARMENIA CARGA S.A. deben cumplir con las recomendaciones y las buenas prácticas en materia de seguridad de la información, establecidas por la dependencia que tenga a cargo la vigilancia y control del buen uso de la tecnología propia de TRANSARMENIA CARGA S.A., incluyendo pero sin limitarse todos los equipos físicos y el sustento lógico que haga parte de la operación del sistema y sus servicios complementarios.
- Los ejecutivos deben revelar cualquier conflicto de intereses respecto a su organización.

Compromiso de los colaboradores con la ética.

- Los colaboradores de TRANSARMENIA CARGA S.A. tratarán a todos de manera justa, primando el respeto mutuo, promoviendo un ambiente de equipo y evitando la intención y la apariencia de prácticas poco éticas o comprometedoras. Cada colaborador necesita aplicar esfuerzo e inteligencia a su procura por mantener los valores éticos.
- Los colaboradores de TRANSARMENIA CARGA S.A. no debe divulgar bajo ninguna circunstancia, la información de la empresa. Esto aplica pero sin limitarse a conversaciones en lugares de trabajo o en tránsito de rutas, con cualquier persona que no esté autorizada para conocer dicha información.
- Los colaboradores dentro de TRANSARMENIA CARGA S.A. deben cumplir con las recomendaciones y las buenas prácticas en materia de seguridad de la información, establecidas por la dependencia que tenga a cargo la vigilancia y control del buen uso de la tecnología propia de TRANSARMENIA CARGA S.A., incluyendo pero sin limitarse todos los equipos físicos y el sustento lógico que haga parte de la operación del sistema y sus servicios complementarios.
- Los colaboradores ayudarán a la organización a aumentar la satisfacción del cliente proporcionando un servicio de calidad y una respuesta oportuna a las consultas que este pueda presentar.
- Los colaboradores deben revelar en el menor término y de forma escrita a su jefe inmediato, cualquier conflicto de intereses en relación con TRANSARMENIA CARGA S.A.
- Los colaboradores deben considerar las siguientes preguntas cuando cualquier comportamiento es cuestionable:

    - ¿Es legal el comportamiento?
    - ¿El comportamiento cumple con todas las políticas apropiadas de TRANSARMENIA CARGA S.A.?
    - ¿Este comportamiento refleja los valores y cultura de TRANSARMENIA CARGA S.A.?

- ¿Podría el comportamiento afectar adversamente a las partes interesadas de la organización?
- ¿Se sentiría personalmente preocupado si el comportamiento apareciera en titulares noticieros?
- ¿Podría el comportamiento afectar negativamente a TRANSARMENIA CARGA S.A., si todos los colaboradores lo hicieran?

M- POLÍTICA DE CONSTRUCCIÓN DE CONTRASEÑAS.

Todas las contraseñas deben cumplir o sobrepasar las siguientes directrices. Las contraseñas fuertes tienen las siguientes características:

- Contienen al menos doce (12) caracteres alfanuméricos.
- Contienen letras en mayúscula y minúsculas.
- Contienen al menos un número (por ejemplo, 0-9).
- Contienen por lo menos uno de los siguientes caracteres especiales: @,!$%^&*()_+|~-=\`{}[]:";'<>?,/.

Las contraseñas débiles tienen las siguientes características:

- Cuentan con menos de 8 caracteres.
- Se encuentra en un diccionario, incluyendo un idioma extranjero, o existe en una lengua, dialecto o jerga.
- Cuentan con información personal como fechas de cumpleaños, direcciones, números telefónicos, o nombres de familiares, mascotas, amigos o personajes de fantasía.
- Tienen información relacionada con el trabajo como nombre del edificio en donde se trabaja, comandos de un sistema, lugares de la empresa y elementos hardware o software.
- Cuentan con patrones numéricos como aaabbb, qwerty, zyxwvuts o 123321.
- Cuentan con palabras comunes deletreadas hacia atrás, precedidas o seguidas por un número (por ejemplo, oterces, secreto1 o 1secreto).
- Utilizan alguna versión de "Bienvenido123", "Contraseña123", "Cambiame123".

Nunca se debe escribir una contraseña por sí mismo. En su lugar, se debe procurar crear contraseñas que no puedan ser recordadas fácilmente y almacenarlas en un almacén de contraseñas. Una forma de hacerlo es crear una contraseña basada en un título de canción, afirmación u otra frase. Por ejemplo, la frase, **"Ojo Esto puede ser una manera de recordar"** podría convertirse en la contraseña **0j0-EpSuMdR!**, ú otra variación. **Importante:** No use ninguno de estos ejemplos como contraseña en sus sistemas de información.

Otra forma de realizar esta construcción de contraseñas es usando generadores aleatorios en línea como http://passwordsgenerator.net/. La Ilustración 1 muestra un ejemplo:

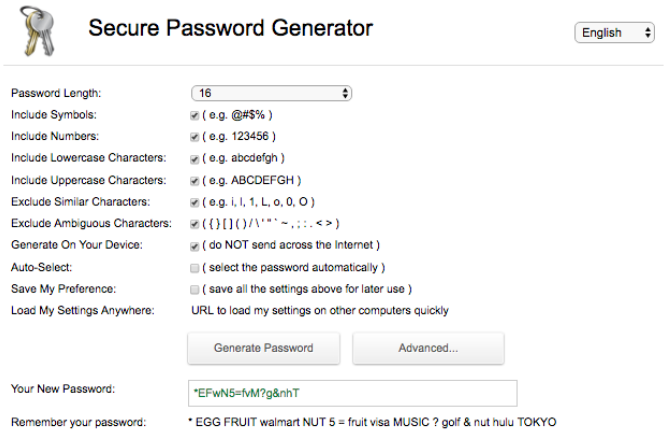

Ilustración 1. Ejemplo de generación de contraseñas en línea

Las frases de contraseñas son usadas generalmente como llaves de autenticación publica/privada. Un sistema de llave publica/privada define una relación matemática entre la llave publica que todos conocen, y la llave privada, la cual solo conoce el propietario. Sin la llave publica para desbloquear la llave privada, el usuario no podrá tener acceso. Una frase de contraseña es similar a una contraseña, sin embargo, es relativamente más extensa y está constituida por múltiples palabras, lo cual provee una mayor seguridad contra los ataques de diccionario. Las frases de contraseña fuertes deben seguir las directrices generales de construcción de contraseñas que incluyan letras mayúsculas y minúsculas, números y caracteres especiales (por ejemplo, **ElTraficoEstuvo*&$Hoy!**).

Se recomienda el uso de almacenes de contraseñas, con el fin realizar una disposición adecuada mediante una contraseña maestra que le permita cifrar las demás contraseñas con un algoritmo robusto y resistente a ataques de fuerza bruta. Es importante aclarar que con el almacén de contraseñas debe tener un especial cuidado de restringir los accesos a las personas no autorizadas con el fin de garantizar la confidencialidad e integridad de la información allí contenida. Un almacén de contraseñas recomendado para el ejercicio es KeyPass por su modelo de licenciamiento de código abierto, cuyo sitio web es http://keepass.info/. Allí podrá encontrar versiones para diferentes plataformas. La Ilustración 2 muestra un ejemplo de su interfaz de usuario.

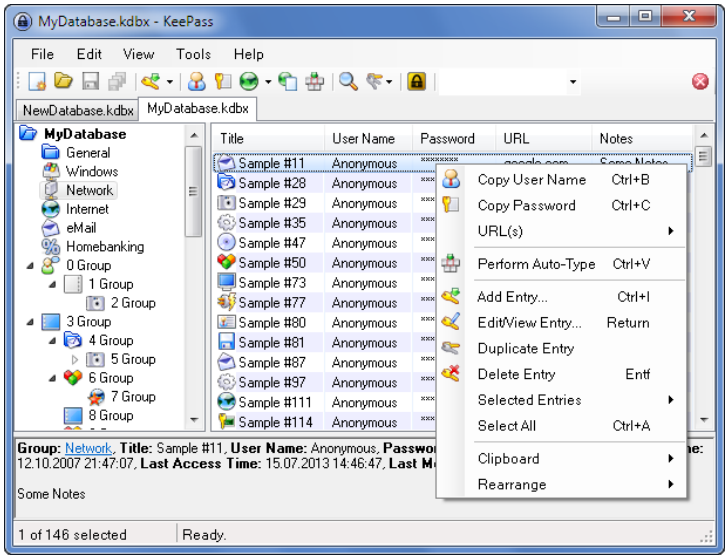

Ilustración 2. Ejemplo de la interfaz de KeyPass

N- POLÍTICA DE PROTECCIÓN DE CONTRASEÑAS.

- Todas las contraseñas de nivel de usuario y de nivel de sistema deben cumplir con la política de construcción de contraseñas.
- Los usuarios no deben usar la misma contraseña para cuentas de TRANSARMENIA CARGA S.A. y para otro acceso ajeno a la organización (por ejemplo, cuenta de ISP personal, comercio de opciones, beneficios, etc.).
- En lo posible, los usuarios no deben usar la misma contraseña para diversas necesidades de acceso a TRANSARMENIA CARGA S.A.
- Cuando se utiliza el Protocolo Simple de Administración de Red o SNMP (del inglés, Simple Network Management Protocol), las cadenas comunes deben definirse como algo distinto a los valores predeterminados de público, privado y sistema, y deben ser diferentes de las contraseñas utilizadas para iniciar sesión de forma interactiva. Las cadenas de SNMP deben cumplir con las directrices de construcción de contraseñas.

•Las contraseñas no deben ser compartidas con nadie, deben ser tratadas como información sensible, confidencial de TRANSARMENIA CARGA S.A., incluyendo pero sin limitarse, asistentes administrativos, secretarios, gerentes, compañeros de trabajo durante las vacaciones y miembros de la familia.
•Las contraseñas no deben insertarse en los mensajes de correo electrónico, ni en ninguna otra forma de comunicación electrónica.
•No revelar las contraseñas por teléfono a nadie, sin importar el mecanismo de presión que se ejerza.
•No revelar la contraseña en cuestionarios o formularios de seguridad.
•No insinúe o de indicios del formato de una contraseña, por ejemplo: "mi apellido".
•No escribir ni guardar las contraseñas en cualquier lugar de su oficina.
•No almacene contraseñas en un archivo de un sistema informático o dispositivos móviles (teléfono, tablet) sin algún tipo de cifrado.
•No utilice la función "Recordar Contraseña" de las aplicaciones, por ejemplo: navegadores web.
•Cualquier usuario que sospeche que su contraseña puede estar comprometida debe informar el incidente y cambiar todas las contraseñas.

Cambio de contraseñas.

•Todas las contraseñas a nivel de sistema (por ejemplo, root, cuentas de administración de aplicaciones, etc.) deben cambiarse al menos trimestralmente.
•Todas las contraseñas a nivel de usuario (por ejemplo, correo electrónico, web, computador de escritorio, etc.) deben cambiarse al menos cada seis meses. El intervalo de cambio recomendado es cada cuatro meses.
•El cruce de contraseñas o las conjeturas pueden realizarse de forma periódica o aleatoria por el equipo de seguridad de la información o sus delegados. Si se detecta una falla o se rompe una contraseña durante una de estas exploraciones, se le solicitará al usuario que la cambie para que cumpla con las directrices de construcción de contraseñas.

Desarrollo de aplicaciones.

Los desarrolladores de aplicaciones deben asegurarse que sus programas contienen las siguientes precauciones de seguridad:

•Deben adoptar soporte en sus aplicaciones para el uso de contraseñas que cumplan con la política para la construcción de contraseñas.
•Las aplicaciones deben soportar autentificación de usuarios individuales, mas no de grupos.
•Las aplicaciones no deben almacenar contraseñas en texto plano o en alguna forma fácil de descifrar.
•Las aplicaciones no deben transmitir las contraseñas en texto plano a través de la red.
•Las aplicaciones deben proporcionar algún tipo de gestión de roles, de modo que un usuario pueda asumir las funciones de otro sin tener que saber su contraseña.
•Se debe permitir el uso de contraseñas y frases de contraseña. Las frases de contraseña se utilizan generalmente para la autenticación de clave pública / privada.
Todas las reglas anteriores que se aplican a las contraseñas se aplican a las frases de contraseña.

Almacenes de contraseñas.

Se recomienda el uso de almacenes de contraseñas, con el fin de realizar una disposición adecuada mediante una contraseña maestra que le permita cifrar las demás contraseñas con un algoritmo robusto y resistente a ataques de fuerza bruta. Es importante aclarar que con el

almacén de contraseñas debe tener un especial cuidado de restringir los accesos a las personas no autorizadas con el fin de garantizar la confidencialidad e integridad de la información allí contenida. Un almacén de contraseñas recomendado para el ejercicio es KeyPass por su modelo de licenciamiento de código abierto, cuyo sitio web es http://keepass.info/. Allí podrá encontrar versiones para diferentes plataformas. La Ilustración 1 muestra un ejemplo de su interfaz de usuario.

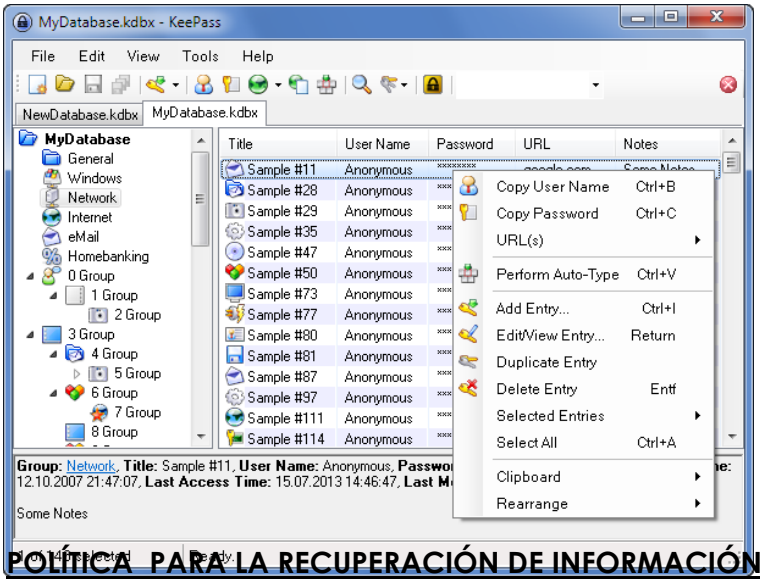

Ilustración 3. Ejemplo de la interfaz de KeyPass

O- POLÍTICA PARA LA RECUPERACIÓN DE INFORMACIÓN ANTE DESASTRES

Hardware

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe adoptar los siguientes criterios para proteger la integridad técnica de la institución.

Cambios al hardware:

- Los equipos computacionales de TRANSARMENIA CARGA S.A. no deben ser alterados ni mejorados (cambios de procesador, memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área responsable.
- Los funcionarios deben reportar a los entes pertinentes de TRANSARMENIA CARGA S.A. sobre daños y pérdida del equipo que tengan a su cuidado y sea propiedad de TRANSARMENIA CARGA S.A. La intervención directa para reparar el equipo debe estar expresamente prohibida. Es deber de la organización el proporcionar personal interno o externo para la solución del problema reportado.
- Todos los equipos de la organización deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.
- Todo el hardware que adquiera la organización debe conseguirse a través de canales de compra estándares.
- Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la empresa, se debe aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.
- Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

- Los equipos computacionales, sean estos estaciones de trabajo, servidores, dispositivos de comunicación, etc., no deben moverse o reubicarse sin la aprobación previa del departamento de sistemas.

Acceso físico y lógico:

- Antes de conectarlos a la red interna todos los servidores de TRANSARMENIA CARGA S.A. deben ser autorizados por el área responsable del hardware.
- Todos los computadores multiusuario y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.
- Las copias de seguridad de la información, discos externos y documentos de soporte se deben ubicar en áreas restringidas en el centro de datos y en sitios alternos con acceso únicamente a personas autorizadas.
- Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.
- Los equipos de computación de TRANSARMENIA CARGA S.A. deben ser protegidos por mecanismos de control aprobados por el departamento de sistemas.
- Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de TRANSARMENIA CARGA S.A. deben ser restringidas.
- Todas las líneas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de que la pantalla de autenticación aparezca en la terminal del usuario.

Respaldo y continuidad del negocio:

- La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.
- Los equipos del centro de datos se deben equipar con unidades suplementarias de energía eléctrica (UPS y Grupo Electrógeno).
- El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único que cause la caída de todos los servicios.
- Las copias de seguridad de los sistemas de información y redes deben ser almacenados en una zona diferente de donde reside la información original. Estas zonas son definidas por el departamento de sistemas de TRANSARMENIA CARGA S.A.
- A todo equipo de cómputo, comunicaciones y demás equipos de soporte se le debe realizar un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.
- Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe ser documentada y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

Otros:

- Los equipos portátiles y móviles de computación que contengan información sensible deben utilizar software de cifrado para proteger la información.
- Todo equipo de cómputo y de comunicaciones de TRANSARMENIA CARGA S.A. debe tener un número (lógico y físico) de identificación permanente grabado en el equipo, además, los inventarios físicos se deben realizar en forma periódica, regular y eficiente.

- Todo equipo portátil debe tener Declaración de Responsabilidad, la cual incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

Software.

Los colaboradores con funciones y responsabilidades para con el software organizacional deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje.

Administración del software:

- La empresa debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato.
- Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada. Igualmente, todo el software y la documentación del mismo que posea la organización incluirán avisos de derechos de autor y propiedad intelectual.
- Todas las aplicaciones se clasificarán en una de las siguientes categorías: Misión Crítica, Prioritaria y Requerida. Para las de misión crítica y prioritaria deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alterno y seguro de custodia.
- Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la organización, se modificarán únicamente por el personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

Adquisición del software:

- El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo.
- El software protegerá los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos.
- Cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema.

Implantación del software:

- Para implantar un software mediará una autorización por escrito del responsable para tal fin.
- Las características que son innecesarias en el ambiente informático se identificarán y desactivarán en el momento de la instalación del software.
- Antes de implementar el software en producción se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción.
- Deberá existir un cronograma de puesta en producción con el fin de minimizar el impacto del mismo.

Mantenimiento del software:

- El área de desarrollos de sistemas no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. A su vez, se

contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

- La documentación de todos los cambios hechos al software se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software, éste deberá firmar un acuerdo de no divulgación y utilización no autorizada del mismo.
- Para cada mantenimiento a la versión del software de misión crítica y prioritaria se actualizará el depositado en custodia en el sitio alterno y el respaldado en la organización. Este software y su documentación se verificarán y certificará su actualización.

P- <u>POLÍTICA PARA LA SEGURIDAD DE LOS DATOS</u>

Con el fin de mantener la seguridad de la información tratada por TRANSARMENIA CARGA S.A., esta política describe el comportamiento que se espera de los colaboradores a la hora de administrar datos y ofrece una clasificación de los tipos de datos con los que deben tener especial cuidado. Asimismo, según las definiciones incluidas en diferentes estándares de cumplimiento y prácticas recomendadas del sector, el cifrado completo de los discos es necesario para evitar la divulgación de los datos si se extravía un activo. En esta política se definen los requisitos del cifrado completo de discos como medida de control, además de los procesos relacionados.

<u>Requisitos específicos.</u>

•Realice los cursos de concienciación sobre seguridad de TRANSARMENIA CARGA S.A. y comprométase a adherirse a la política de uso aceptable.
•Las personas que visiten TRANSARMENIA CARGA S.A. deben estar acompañadas por algún colaborador autorizado en todo momento. Si está encargado de acompañar a las visitas, diríjalas solamente a las zonas adecuadas.
•No está permitido hacer referencia a temas o datos delicados y confidenciales en público o a través de sistemas o canales de comunicación no controlados por la organización. Por ejemplo, está prohibido utilizar sistemas externos de correo electrónico no alojados por TRANSARMENIA CARGA S.A. para la distribución de datos.
•Mantenga su escritorio organizado. Para conservar la seguridad de la información, no deje ningún dato englobado en esta política sin atender encima del escritorio.
•Según la política para la construcción de contraseñas, deberá utilizar una contraseña segura en todos los sistemas de la organización. Dichas credenciales deben ser exclusivas y no deben utilizarse en otros sistemas o servicios externos.
•Al finalizar el contrato, los colaboradores deberán devolver todos los registros (en cualquier formato) que contengan información personal.
•Si se produce el extravío de cualquier dispositivo que contenga datos englobados en esta política (por ejemplo, teléfonos móviles, portátiles, etc.), informe de inmediato al equipo de seguridad informática.
•Si sospecha que algún sistema o proceso no cumple la política o pone en peligro la seguridad de la información, tiene el deber de informar al departamento de sistemas para que se tomen las medidas necesarias.
•Si se le ha concedido la capacidad de trabajar de forma remota, tome medidas de precaución adicionales para asegurarse de que maneja los datos adecuadamente. Solicite ayuda al equipo de seguridad informática si no está seguro de sus responsabilidades.
•Las transferencias de datos dentro de TRANSARMENIA CARGA S.A. deben realizarse solamente a través de los mecanismos seguros proporcionados por la empresa (por ejemplo,

correo electrónico, recursos compartidos, memorias USB cifradas, etc.). La organización le proporcionará los sistemas o dispositivos correspondientes para tal fin. No utilice otros mecanismos para el manejo de datos englobados en esta política. Si tiene alguna pregunta relacionada con el uso de cualquier mecanismo de transferencia o detecta alguno que no cumpla los requisitos empresariales, informe al equipo de seguridad informática.

•Toda información transferida a cualquier dispositivo móvil (por ejemplo, memorias USB u ordenadores portátiles) debe estar cifrada de acuerdo con las prácticas recomendadas del sector, y las leyes y normativas correspondientes. Si tiene alguna duda sobre los requisitos, solicite ayuda al equipo de seguridad informática.

Q- POLÍTICA PARA LAS CREDENCIALES DE LAS BASES DE DATOS

Con el fin de mantener la seguridad de las bases de datos internas de TRANSARMENIA CARGA S.A., el acceso por programas de software debe ser otorgado sólo después de la autenticación con credenciales. Las credenciales utilizadas para esta autenticación no deben residir en el código fuente del programa en texto claro. Las credenciales de base de datos no deben almacenarse en una ubicación a la que se pueda acceder a través de un servidor web.

Requisitos específicos.

Almacenamiento de nombres de usuario y contraseñas de base de datos.

•Los nombres de usuario y contraseñas de la base de datos pueden almacenarse en un archivo separado del código fuente del programa, este archivo no debe ser accedido para lectura y/o escritura por un usuario no autorizado.

•Las credenciales de acceso pueden residir en el servidor de la base de datos. Para este caso un número de comprobación (hash) puede ser almacenado en el código fuente del programa.

•Las credenciales de acceso a la base de datos pueden ser almacenadas como parte de un servidor de autenticación (es decir, un directorio de derechos), como un servidor LDAP utilizado para la autenticación de usuarios.

•La autenticación de la base de datos puede ocurrir en nombre de un programa como parte del proceso de autenticación del usuario en el servidor de autenticación. En este caso, no hay necesidad de programar el uso de credenciales de acceso a la base de datos.

•Las credenciales de la base de datos pueden no residir en el árbol de documentos de un servidor web.

•La autenticación de paso (es decir, la autenticación de Oracle OPS $) no debe permitir el acceso a la base de datos basada únicamente en la autenticación de un usuario remoto en el host remoto.

•Las contraseñas o frases utilizadas para acceder a una base de datos deben cumplir con la política para la construcción de contraseñas.

Recuperación de nombres de usuario y contraseñas de la base de datos.

•Si se almacena en un archivo que no es código fuente, los nombres de usuario y las contraseñas de la base de datos se deben leer del archivo inmediatamente antes de su uso. Inmediatamente después de la autenticación de la base de datos, se debe liberar o borrar la memoria que contiene el nombre de usuario y la contraseña.

•El ámbito en el que puede almacenar credenciales de base de datos debe estar físicamente separado de las otras áreas de su código, por ejemplo, las credenciales deben estar en un archivo de origen independiente.
•El archivo que contiene las credenciales no debe contener ningún otro código excepto las credenciales (es decir, el nombre de usuario y la contraseña) y cualquier función, rutina o método que se utilizará para acceder a las credenciales.

R- <u>POLÍTICA PARA MEDIOS EXTRAIBLES</u>

•El personal de TRANSARMENIA CARGA S.A. sólo puede utilizar medios extraíbles en sus equipos de trabajo aprobados por el departamento de sistemas.
•Estos medios extraíbles no se pueden conectar o utilizar en equipos que no estén bajo la calidad de propiedad o arrendamiento de TRANSARMENIA CARGA S.A., a no ser que sea autorizado su uso por autorización escrita y explícita del personal a cargo.
•La información confidencial debe ser almacenada en medios extraíbles sólo cuando se requiera, bajo la responsabilidad de un usuario en el desempeño de sus deberes asignados o al proporcionar información requerida por una agencia gubernamental.
•Cuando la información confidencial se almacene en medios extraíbles, esta debe contar con un mecanismo de cifrado de acuerdo con la política de cifrado aceptada por TRANSARMENIA CARGA S.A.

•Las excepciones a esta política pueden ser solicitadas caso por caso a TRANSARMENIA CARGA S.A. que evaluará cada uno de acuerdo a sus procedimientos de excepción previamente establecidos.
•El departamento de sistemas será el encargado de establecer los mecanismos de control y monitoreo para evitar que los demás colaboradores usen dispositivos extraíbles sin la previa autorización y estará facultado para inhabilitar los puertos de conexión de forma física o lógica, según sea la necesidad.