MANUAL INTERNO DE POLITICAS Y PROCEDIMIENTOS PARA EL-TRATAMIENTO DE DATOS PERSONALES

CENTRO DE FORMACION Y ESTUDIOS EN LIDERAZGO Y GESTION S.A.S.

NIT 900156547-1

Author: TimeCentury S.A.S | Cyber Security Advisory |
info@TimeCentury.com | www.TimeCentury.com.

Version: V1.6, 28 de junio 2017

Prevent | Defend | Analyse

Índice

1 NOMBRE E IDENTIFICACIÓN DE LA EMPRESA 3
2 NORMATIVIDAD APLICABLE 3
3 DEFINICIONES 3
4 DERECHOS DEL TITULAR DE LOS DATOS 4
5 DEBERES DE LA EMPRESA COMO RESPONSABLES DE LA INFORMACIÓN 5
6 PROCEDIMIENTO Y CANALES PARA LA ATENCION DE SOLICITUDES CONSULTAS Y RECLAMOS 5
7 MEDIDAS DE SEGURIDAD 6
8 VIGENCIA 6
9 PROGRAMA A NIVEL DIRECTIVO, MANUAL INTERNO 6
9.1 POLITICA DE SEGURIDAD DE ALMACENAMIENTO ELECTRONICO 6
9.2 POLITICA DE DESTRUCCION DE INFORMACION 7
9.3 POLITICA DE AUDITORIA 7
9.4 POLITICA PARA TERCEROS 7
9.5 POLITICA DE PROTECCIÓN DE LA INFORMACIÓN A TRAVÉS DEL USO DE EQUIPOS MULTIFUNCIONALES (IMPRESORA, FOTOCOPIADORA, ESCÁNER Y FAX) 7
9.6 TRATAMIENTO DE DATOS DE MENORES 8
10 BASES DE DATOS 8
10.1 EMPLEADOS 8
10.2 PROVEEDORES 8
10.3 CLIENTES 9
10.4 ESCUELA LIDERAZGO 9
10.5 FOROS 9
10.6 E-LEARNING 9
10.7 SOCIOS 9
11 GESTION DE RIESGOS 10
12 DATOS RECOLECTADOS ANTES DE JUNIO DE 2013 art. 9 11
13 PLAZO PARA IMPLEMENTAR LA PROTECCION DE DATOS 12
14 RESPONSABILIDAD 12

1 NOMBRE E IDENTIFICACIÓN DE LA EMPRESA

CENTRO DE FORMACION Y ESTUDIOS EN LIDERAZGO Y GESTION S.A.S.,
NIT 900.156.547-1,
DIRECCION CALLE 100 # 8A-55 TORRE C OFICINA 704 BRR CHICO,
Bogotá, Cundinamarca Teléfono(1) 6167311
Email msierra@clg.com.co

2 NORMATIVIDAD APLICABLE

El presente documento da cumplimiento a la Ley 1581 de 2012 ("Por la cual se dictan disposiciones generales para la protección de datos personales") y el Decreto 1377 de 2013 ("Por el cual se reglamenta parcialmente la Ley 1581 de 2012").

3 DEFINICIONES

- **Titular**: Persona física cuyos datos sean objeto de Tratamiento. Respecto de las personas jurídicas se predica el nombre como derecho fundamental protegido constitucionalmente.
- **Usuario**: Es la persona natural o jurídica que tiene interés en el uso de la información de carácter personal.
- **Dato personal**: Es cualquier Dato y/o información que identifique a una persona física o la haga identificable. Pueden ser Datos numéricos, alfabéticos, gráficos, visuales, biométricos, auditivos, perfiles o de cualquier otro tipo.
- **Datos Personales Sensibles**: Categoría de carácter personal especialmente protegida, por tratarse de datos relacionados con la intimidad del Titular o cuyo uso indebido puede generar discriminación. Son, entre otros, aquellos concernientes a la salud, sexo, orientación política, raza pertenencia a sindicatos, huellas biométricas o/y origen étnico, etc.
- **Dato público**: todos aquellos datos que no sean semiprivados, privados o sensibles de conformidad con la Ley 1581 de 2012. 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, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones y procedimientos técnicos de carácter automatizado o no que se realizan sobre Datos Personales, tales como la recolección, grabación, almacenamiento, conservación, uso, circulación, modificación, bloqueo, cancelación, entre otros.
- **Base de Datos Personales**: Es todo conjunto organizado de Datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Cesión de base de Datos**: Tratamiento de Datos que supone su revelación a una persona diferente al titular del Dato o distinta de quien estaba habilitado como cesionario.
- **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, 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.
- **Responsable del Tratamiento**: Es la persona natural o jurídica, de naturaleza pública o privada, que recolecta los Datos Personales y decide sobre la finalidad, contenido y uso de la base de Datos para su Tratamiento.
- **Encargado del Tratamiento**: Es la 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.
- **Custodio de la Base de Datos**: Es la persona física que tiene bajo su custodia la base de Datos Personales al interior de la empresa.
- **Habeas Data**: Derecho fundamental de toda persona para conocer, actualizar, rectificar y/o cancelar la información y Datos Personales que de ella se hayan recolectado y/o se traten en bases de Datos públicas o privadas, conforme lo dispuesto en la Ley y demás normatividad aplicable.
- **Violación de Datos Personales**: Es el delito creado por la ley 1273 de 2009, contenido en el artículo 269 F del Código Penal Colombiano. La conducta prohibida es la siguiente: "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, Datos Personales contenidos en base de Datos, archivos, bases de Datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".
- **Violaciones de las Medidas de Seguridad de los Datos Personales**: Será considerado incidente de seguridad aquella situación que implique una violación de las medidas de seguridad adoptadas por la empresa para proteger los Datos Personales entregados para su custodia, sea como Responsable y/o Encargado del Tratamiento, así como cualquier otra conducta que constituya un Tratamiento inadecuado de Datos Personales en contravía de lo aquí dispuesto o de lo señalado en la Ley. Todo incidente de seguridad que comprometa los Datos Personales en poder la empresa deberá ser informado a la autoridad de control en la materia.

4 DERECHOS DEL TITULAR DE LOS DATOS

1. A conocer, actualizar y rectificar sus datos personales ante los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer entre otros, referente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
2. A solicitar prueba de la autorización otorgada al Responsable del Tratamiento.

   Nota: Hay casos en que expresamente se exceptúa la autorización requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

3. A Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les haya dado a sus datos personales.
4. A Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.

5. A 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. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
6. A Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
7. A ser informado sobre el procedimiento y el contacto de la persona o área responsable de la atención de peticiones, consultas y reclamos, ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir datos; y a revocar la autorización.

5 DEBERES DE LA EMPRESA COMO RESPONSABLES DE LA INFORMACIÓN

1. Garantizar al titular, el derecho que le asiste en el cumplimiento de Hábeas Data.
2. Solicitar y conservar, la copia de la autorización otorgada por el Titular.
3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Rectificar la información en caso necesario y comunicar lo pertinente a cada encargado del Tratamiento de información.
6. Tramitar las consultas y reclamos formulados en los términos señalados en la Ley 1581 de 2012.

6 PROCEDIMIENTO Y CANALES PARA LA ATENCION DE SOLICITUDES CONSULTAS Y RECLAMOS

El titular o la persona autorizada podrá formular solicitudes o consultas a través de:

1. Línea de atención al cliente: (1)6227663
2. Requerimiento escrito: CR 11A # 93-67 OF 505 BRR CHICO, Bogotá, Cundinamarca
3. Email: mrincon@clg.com.co

La consulta será atendida en un término máximo de 10 días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuera posible atender la consulta dentro del término antes indicado la empresa lo expresará así al interesado, señalando la fecha en que se atenderá su consulta.

7 MEDIDAS DE SEGURIDAD

La empresa adoptará las medidas necesarias de seguridad tales como contraseñas a los sistemas, políticas de acceso a archivos fisicos o digitales, intalación de antivirus, firewalls a los sistemas, controles de acceso al establecimiento para garantizar la seguridad de la base de datos personales evitando así uso no autorizado, adulteración o pérdida.

8 VIGENCIA

El presente manual rige a partir del veinte (28) de junio de 2017

9 PROGRAMA A NIVEL DIRECTIVO, MANUAL INTERNO

Con el fin de dar un debido cuidado al tratamiento de la información, la gerencia hace un seguimiento semestral a las normativas implementadas.

9.1 POLITICA DE SEGURIDAD DE ALMACENAMIENTO ELECTRONICO

La empresa se encarga de realizar actualizaciones de los programas de sistema operativo y de contabilidad, de esta manera el antivirus se va actualizando, igualmente tener un cortafuego (firewall) al día.

Se implementará un sistema de identificación de usuarios con su respectiva clave la cual permite un eventual monitoreo de ser necesario. De la misma manera con el fin de proteger la información se debe bloquear la pantalla del computador con clave para que la información solo esté disponible cuando se está trabajando en el mismo.

La contraseña se debe cambiar periódicamente idealmente cada 3 meses, el sistema se programara para exigir a los usuarios sustituir la clave, de lo contrario no les permitirá el acceso.

Complejidad de la clave: contener un mínimo de 8 caracteres, que contenga al menos: un carácter especial, un número, una mayúscula y una minúscula.

Copia de seguridad: además de la copia generada automáticamente por el servidor se debe hacer una copia en un disco externo semanal, el cual debe reposar en la empresa bajo llave en un archivador, en un lugar lejano al servidor o si es posible en un lugar diferente a la sede de la empresa.

En caso de ser necesario el envío electrónico de archivos que contengan datos sensibles y confidenciales, deben estar encriptados con el programa VeraCrypt.

9.2 POLITICA DE DESTRUCCION DE INFORMACION

La administración de la empresa es consciente de la prudencia y responsabilidad en el momento de deshacerse de los datos. Por lo tanto, para la data física se hace una destrucción manual y para la electrónica un borrado seguro electrónico (aconsejado por su administrador de sistemas).

Eliminación permanente: Se trata de reemplazar o sobrescribir automáticamente, la información sensible, en lugar de simplemente borrarla. Un software de borrado confiable además de borrar el contenido, reescribe sobre cada palabra, automáticamente.

9.3 POLITICA DE AUDITORIA

Se deben efectuar controles y verificación del cumplimiento de las políticas establecidas; cada 6 meses. De dicha auditoría se emitirá un informe del cumplimiento de los lineamientos internos con el objeto de hacer los reajustes en caso de ser necesarios. Igualmente realizar capacitaciones que sensibilicen a los empleados sobre los riesgos inherentes al entorno digital.

9.4 POLITICA PARA TERCEROS

En el evento de ceder las bases de datos en su totalidad o parcialmente a un tercero, la empresa tiene como compromiso revisar las políticas de protección de datos que maneja la compañía a quien se le comparte la información de los titulares. Se deja constancia con los respectivos documentos que soporten que la responsabilidad hacia los titulares y el tratamiento que se les da a los datos, recae sobre la compañía tercerizadora.

9.5 POLITICA DE PROTECCIÓN DE LA INFORMACIÓN A TRAVÉS DEL USO DE EQUIPOS MULTIFUNCIONALES **(IMPRESORA, FOTOCOPIADORA, ESCÁNER Y FAX).**

Los empleados deben tener en cuenta las siguientes consideraciones cuando impriman documentos a través de los equipos multifuncionales e impresoras que se encuentran dentro de las instalaciones de la empresa o que son propiedad de este:

1. Se prohíbe el uso de copias de documentos que contengan información personal o datos confidenciales y se destinen con fines de reciclaje.
2. Recoger inmediatamente todos los faxes, impresiones y/o fotocopias que contengan información confidencial para evitar su revelación.
3. Se debe imprimir solo lo que es estrictamente necesario.
4. Verificar el equipo multifuncional o impresora y las áreas adyacentes para asegurarse de que no queden copias adicionales. Si encuentra copias adicionales se deben destruir. (El uso de trituradores de papel es recomendado)
5. Los empleados deben asegurarse que tienen el documento original antes de retirarse del equipo multifuncional o de la impresora.

6. Si el equipo multifuncional o la impresora no están funcionando, borre el archivo de impresión.
7. Verificar el número al que se enviará el fax antes de hacerlo, para evitar él envió de documentos a números equivocados.

9.6 TRATAMIENTO DE DATOS DE MENORES

CENTRO DE FORMACION Y ESTUDIOS EN LIDERAZGO Y GESTION S.A.S., solo trata datos personales de menores de edad cuando sean necesarios y estos sean de naturaleza pública o provengan de la información suministrada por empleados o contratistas, al momento de su vinculación laboral o de prestación de servicios a la empresa.

Lo mencionado, dará conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y, cuando el tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, la empresa exigirá al representante legal o tutor del niño, niña o adolescente, la autorización del menor, previo a que el menor de su opinión frente al tratamiento que se le dará a sus datos, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto, tal como lo indica la Ley 1581. CENTRO DE FORMACION Y ESTUDIOS EN LIDERAZGO Y GESTION S.A.S. y cualquier persona involucrada en el tratamiento de los datos personales de niños, niñas y adolescentes, velaran por el uso adecuado de los mismos.

En cumplimiento de lo anterior, se aplican y desarrollan los principios y obligaciones establecidos en la Ley 1581 de 2012 y el Decreto 1377 de 2013.

10 BASES DE DATOS

10.1 EMPLEADOS

Hojas de vida e información personal (físico): información usada para afiliaciones de empleados a seguridad social usando la página de los proveedores y demás asuntos pertinentes para contratación, hacer seguimiento en los procesos de promoción y evaluación del personal, actividades de bienestar y son almacenada en carpetas identificadas en un archivador bajo llave. Estas carpetas son solo manejadas por la encargada de nómina y/o el Representante Legal. Terminada la relación laboral se almacenan los archivos en el mismo lugar rotulado como Empleados retirados.

La información también se almacena electrónicamente en el servidor

10.2 PROVEEDORES

Datos que reposan en la base: Nombre, documento de identidad, RUT, Certificado de Cámara de Comercio, teléfono, dirección, cuenta bancaria

La información se almacena electrónicamente en el servidor y en físico con carpetas debidamente marcadas, las cuales reposan en un archivador bajo llave.

10.3 CLIENTES

Datos de clientes crédito: Nombre, documento de identidad, teléfono, dirección, Cámara de Comercio, RUT y pagaré firmado por el cliente.

Cliente contado: No se obtiene información alguna de ellos.

La información se almacena electrónicamente en el servidor y en físico con carpetas debidamente marcadas, las cuales reposan en un archivador bajo llave. Se usa para dar a conocer eventos, torneos, convenios, promociones, así como para generar una comunicación óptima en relación con nuestros productos y servicios

10.4 ESCUELA LIDERAZGO

Datos que reposan en la base: Nombre, documento de identidad, RUT, teléfono, dirección.

Almacenados electrónicamente

10.5 FOROS

Datos que reposan en la base: Nombre, documento de identidad, firma.

Almacenados electrónicamente, RUT

10.6 E-LEARNING

Datos que reposan en la base: Nombre, documento de identidad, firma. Almacenados electrónicamente

10.7 SOCIOS

Datos que reposan en la base: Nombre, documento de identidad, RUT, certificado de cámara de comercio teléfono, dirección.

Almacenados electrónicamente

11 GESTION DE RIESGOS

La Empresa tiene conocimiento de la existencia de los riesgos de seguridad cibernética e informática, los cuales pueden presentarse en cualquier momento. No existe un plan de riesgo establecido sin embargo se siguen lineamientos tales como el reporte al grupo de respuesta a emergencias cibernéticas de Colombia colCERT, en su sitio web www.colcert.gov.com, lo anterior en caso de que la compañía sea blanco de un ataque cibernético.

En caso de observar que la información personal haya sido manipulada en forma incorrecta la empresa contactara a la SIC http://sic.gov.co para dar aviso de esta conducta.

Manejo de riesgos también implica el establecimiento de un plan de contingencia para incidentes en una eventualidad como puede ser fuego, la pérdida de un computador, descargue no intencional de un malware entre otros, para los cuales debe existir una estrategia de prevención.

El cuadro siguiente toma como referencia dos sucesos, sus implicaciones y el manejo adecuado.

					Cálculo del riesgo			
No.	RIESGO	Como se mitiga el riesgo actualmente	**Impacto:** 1 Moderado 2 Significativo 3 Catastrófico	**Probabilidad** 1 Bajo 2 Medio 3 Alto	**Grado de riesgo**	Reducción de riesgos	Persona responsable	Fecha terminación
1	Pérdida de Computador	Inicio de sesión con usuario y contraseña	3	3	**9**	- Encriptación de disco duro - Respaldo de seguridad	Jefe de seguridad de la información	20.12.2016
2	Incendio	Extinguidor	3	2	**6**	- Detectores de humo - Servidor adicional externo de la organización - Respaldo de seguridad	Jefe de Seguridad física / Consultor de seguridad externa	20.12.2016

12 DATOS RECOLECTADOS ANTES DE JUNIO DE 2013 art. 9

Decreto 1377 de 2013 Artículo 2.2.2.25.2.7. Para estos los datos se tendrá en cuenta lo siguiente:

1. Los responsables deberán solicitar la autorización de los titulares para continuar con el Tratamiento de sus datos personales del modo previsto en el artículo 2.2.2.25.2.4., a través de mecanismos eficientes de comunicación, así como poner en conocimiento de estos sus políticas de Tratamiento de la información y el modo de ejercer sus derechos.
2. Para efectos de lo dispuesto en el numeral 1, se considerarán como mecanismos eficientes de comunicación aquellos que el responsable o encargado usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos.
3. Si los mecanismos citados en el numeral 1 imponen al responsable una carga desproporcionada o es imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos, el Responsable podrá implementar mecanismos alternos para los efectos dispuestos en el numeral 1, tales como diarios de amplia circulación nacional, diarios locales o revistas, ***páginas de Internet*** del responsable, carteles informativos, entre otros, e informar al respecto a la Superintendencia de Industria y Comercio, dentro de los cinco (5) días siguientes a su implementación. Con el fin de establecer cuándo existe una carga desproporcionada para el responsable se tendrá en cuenta su capacidad económica, el número de titulares, la antigüedad de los datos, el ámbito territorial y sectorial de operación responsable y el mecanismo alterno de comunicación a utilizar, de manera que el hecho de solicitar el consentimiento a cada uno de los Titulares implique un costo excesivo y que ellos comprometa la estabilidad financiera del responsable, la realización de actividades propias de su negocio o la viabilidad de su presupuesto programado.

   A su vez se considerará que existe una imposibilidad de solicitar a cada titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos cuando el responsable no cuente con datos de contacto de los titulares, ya sea porque los mismos no obran en sus archivos, registros o bases de datos, o bien, porque estos se encuentran desactualizados, incorrectos, incompletos o inexactos.

4. Si en el término de treinta (30) días hábiles, contado a partir de la implementación de cualesquiera de los mecanismos de comunicación descritos en los numerales 1, 2 y 3 el Titular no ha contactado al Responsable o Encargado para solicitar la supresión de sus datos personales en los términos del presente capítulo, el responsable y encargado podrán continuar realizando el Tratamiento de los datos contenidos en sus bases de datos para la finalidad o finalidades indicadas en la política de Tratamiento de la información, puesta en conocimiento de los titulares mediante tales mecanismos, sin perjuicio de la facultad que tiene el Titular de ejercer en cualquier momento su derecho y pedir la eliminación del dato.
5. En todo caso el Responsable y el Encargado deben cumplir con todas las disposiciones aplicables de la Ley 1581 de 2012 y el presente capítulo. Así mismo, será necesario que la finalidad o finalidades del Tratamiento vigentes sean iguales, análogas o compatibles con aquella o aquellas para las cuales se recabaron los datos personales inicialmente.

Parágrafo. La implementación de los mecanismos alternos de comunicación previstos en esta norma deberá realizase a más tardar dentro del mes siguiente de la publicación del Decreto 1377 de 2013.

13 PLAZO PARA IMPLEMENTAR LA PROTECCION DE DATOS

La Ley 1581 del 17 de Octubre de 2012, en su artículo 28 estableció un plazo de 6 meses para aplicar y adaptar de políticas por parte de las empresas que hagan las veces de encargados y/o responsables del tratamiento de datos.

14 RESPONSABILIDAD

Por todo lo anterior, CENTRO DE FORMACION Y ESTUDIOS EN LIDERAZGO Y GESTION S.A.S. se declara responsable de las presentes políticas y del tratamiento de protección de datos que en sus funciones desarrolle frente a las personas naturales, titulares de datos de carácter personal.