MANUAL DE POLÍTICAS Y PROCEDIMIENTO PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA CONSTRUCTORA BERLÍN S.A.S.

FUNDAMENTO LEGAL

Este manual tiene como finalidad regular los procedimientos de recolección, manejo y tratamiento de los datos de carácter personal que realiza CONSTRUCTORA BERLIN S.A.S, a fin de garantizar y proteger el derecho fundamental de habeas data en el marco de lo establecido en la Ley.1581 de 2012, la cual señala el deber de "adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos"; y de acuerdo con los establecido en el Decreto 1377 de 2013.

DEFINICIONES

De conformidad con la Ley 1581 de 2012 y el Decreto 1377 de 2013, para los efectos del presente manual se deben tener en cuenta las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar acabo el tratamiento de datos personales, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.
- **Base de** Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **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.
- **Base de Datos Automatizada:** Es el conjunto organizado de datos de carácter personal que son creados, tratados y/o almacenados a través de programas de ordenador o software.
- **Base de Datos no Automatizada:** Es el conjunto organizado de datos de carácter personal que son creados, tratados y/o almacenados de forma manual, con ausencia de programas de ordenador o software.
- **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, auditivos o de cualquier otro tipo.
- **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.
- **Dato sensible:** Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **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.
- **Habeas Data:** Derecho fundamental de toda persona para conocer, actualizar, rectificar y/o cancelar la información y Dato personal 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.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Transferencia de Datos Personales:** 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 de Datos Personales:** La transmisión de datos personales por su parte implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **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.
- **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 punible 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

OBJETO

El presente Manual Interno de Políticas y Procedimientos para la Protección de Datos Personales tiene como finalidad adoptar y establecer las reglas aplicables con relación a la recolección, manejo y tratamiento de los datos de carácter personal que realiza CONSTRUCTORA Berlín S.A.S en desarrollo de su objeto social, bien sea en calidad de Responsable y/o Encargado del tratamiento.

DESTINATARIOS

El presente Manual Interno de Políticas y Procedimientos para la Protección de Datos Personales se aplicará y consecuentemente impone el deber de cumplimiento a las siguientes personas:

- Representantes Legales y/o miembros de la Junta Directiva de la Constructora Berlín S.A.S.
- Personal interno de la Constructora Berlín S.A.S que custodien y traten bases de Datos Personales
- Contratistas y personas naturales o jurídicas que presten sus servicios a Constructora Berlín S.A.S bajo cualquier tipo de modalidad contractual, en virtud de la cual se realice cualquier tratamiento de Datos Personales
- Los revisores fiscales que realicen cualquier tratamiento de Datos Personales
- Personas públicas y privadas en condición de titulares de los Datos Personales
- Las demás personas que establezca la Ley

PRINCIPIOS APLICABLES

- Legalidad: Los- procedimientos de recolección, manejo y tratamiento de Datos Personales deben sujetarse a lo establecido en la Ley y en las demás disposiciones que desarrollen la materia.
- Libertad: El tratamiento deberá llevarse a cabo con el consentimiento del titular, adicionalmente los datos personales no podrán ser obtenidos o divulgados sin la autorización del titular, o en ausencia de mandato legal o judicial que revele el consentimiento.
- Veracidad: Los Datos Personales recolectados por Constructora Berlín S.A.S deben ser veraces, completos, exactos, actualizados y comprensibles.
- Transparencia: Constructora Berlín S.A.S velará porque el titular de los Datos Personales pueda obtener, en cualquier momento y sin restricciones, información acerca dela existencia de sus datos.
- Acceso y Circulación Restringida: Los datos personales, salvo los que tengan naturaleza pública, no podrán estar disponibles en internet o en otros medios de- divulgación o comunicación masiva. Cada vez que el titular lo requiera podrá consultar o solicitar que actualicen y rectifiquen sus datos personales.
- Confidencialidad: Las personas que intervengan en el tratamiento de los datos personales, deberán garantizar la reserva de la información, inclusive después de finalizada la relación contractual con la sociedad.

FINALIDAD DEL TRATAMIENTO

Sin perjuicio de lo establecido para cada tipo de base de datos personales que maneja La Empresa, la finalidad de tratamiento de datos personales se sujetará a lo dispuesto en este acápite. En consecuencia, el tratamiento de datos personales realizados por Constructora Berlín S.A.S. será:

a. Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información.
b. Realizar invitaciones a eventos y ofrecer nuevos productos y servicios
c. Gestionar trámites (solicitudes, quejas, reclamos)
d. Efectuar encuestas de satisfacción respecto de los bienes y servicios ofrecidos por Constructora Berlín S.A.S.

e. Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual se contraten estos servicios para la ejecución de las mismas.
f. Contactar al Titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.
g. Contactar al Titular a través de medios electrónicos – SMS o chat para el envío de noticias relacionadas con campañas de fidelización o mejora de servicio.
h. Contactar al Titular a través de correo electrónico para el envío de extractos, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes.
i. Dar cumplimiento a las obligaciones contraídas por Constructora Berlín S.A.S. con el Titular de la Información, con relación al pago de salarios, prestaciones sociales y demás retribuciones consagradas en el contrato de trabajo o según lo disponga la ley (cuando se trate del caso de personal vinculado).
j. Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios (hijos, cónyuge, compañero permanente).
k. Prestar los servicios ofrecidos por Constructora Berlín S.A.S. y aceptados en el contrato suscrito.
l. Suministrar la información a terceros como SINCOSOFT S.A.S. y/o GRUPO TSM INGENIERÍA S.A.S. cuando sea necesario entregarles la información para su debido almacenamiento de acuerdo a lo establecido en esta política.
m. En el caso de empleados, trabajadores o dependientes, suministrar la información para el trámite de incapacidades (EPS), reporte de accidentes de trabajo (ARL), afiliaciones y desafiliaciones en materia pensional (AFP) y cualquier otro trámite necesario para dar cumplimiento a las exigencias laborales o de personal a cargo.

ENCARGADOS DEL TRATAMIENTO

Constructora Berlín S.A.S. con el fin de garantizar la seguridad de su información y hacer uso del aprovechamiento tecnológico, ha contratado con terceras personas el recaudo de los datos personales que los titulares autorizan a La Empresa para realizar el tratamiento, así como también para almacenarlos en servidores externos y suficientemente seguros. Estos encargados son:

IDENTIFICACIÓN: SINCOSOFT S.A.S.
UBICACIÓN: Calle 81 No. 11-08 piso 10 Edificio 8111 – Bogotá D.C - Colombia.
CONTACTO: (datos_personales@sinco.com.co) PBX: (571) 443 0820

IDENTIFICACIÓN: GRUPO TSM INGENIERÍA S.A.S.
UBICACIÓN: Carrera 71 D No. 66B-34 – Bogotá D.C - Colombia.
CONTACTO: administracion@grupotsmingenieria.com

IDENTIFICACIÓN: INFOLAFT SAS
UBICACIÓN: Carrera 71 6 14 torre B oficina 501– Bogotá D.C - Colombia.
CONTACTO: comunicaciones@infolaft.com

IDENTIFICACIÓN: SINCOSOFT S.A.S. - SOFTWARE BITÁKORA
UBICACIÓN: Calle 81 No. 11-08 piso 10 Edificio 8111 – Bogotá D.C - Colombia.
CONTACTO: (juridico@sinco.com.co – augusto@sinco.com.co)
PBX: (571) 443 0820

IDENTIFICACIÓN: DISPAPELES SAS
UBICACIÓN: CALLE 103 69 53– Bogotá D.C - Colombia.
CONTACTO: contacto@dispapeles.com https://dispapeles.com/contacto/

IDENTIFICACIÓN: SAPHETY TRANSSACIONES ELECTRONICAS S.A.S
UBICACIÓN: Calle 97a #9-45 - Edifício Strategic 97 Oficina 207 Bogotá Colombia
CONTACTO: comercial.colombia@saphety.com

DEBERES DEL RESPONSABLE DEL TRATAMIENTO

Los deberes de CONSTRUCTORA BERLIN S.A.S. como Responsable del Tratamiento son:

a) Garantizar al titular en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar 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 y/o pérdida, así como la 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.
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 el presente manual.
k) Informar a solicitud del titular sobre el uso dado a sus datos.

Los datos personales a los que tiene acceso CONSTRUCTORA BERLÍN S.A.S deben ser utilizados únicamente para los fines y propósitos empresariales de CONSTRUCTORA BERLÍN S.A.S, siempre de acuerdo con el alcance de la autorización entregada por el titular.

DEBERES DEL ENCARGADO DEL TRATAMIENTO

Los deberes de los Encargados del Tratamiento de datos personales conforme a la presente política son los siguientes:

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 en los términos del presente reglamento.
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 los términos del presente reglamento.
f) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio
g) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
h) 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.
i) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

DERECHOS DEL TITULAR

De conformidad con lo establecido en el artículo 8 de la Ley 1581 de 2012, el titular de los datos personales tiene los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a LA CONSTRUCTORA BERLÍN S.A.S, en su condición de responsable del tratamiento.
b) Solicitar prueba de la autorización otorgada a LA CONSTRUCTORA BERLÍN S.A.S, en su condición de Responsable del Tratamiento.
c) Ser informado por LA CONSTRUCTORA BERLÍNS.A. S 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, una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento.
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 personares que hayan sido objeto de Tratamiento.
g) El titular de los Datos Personales puede presentar en cualquier momento quejas y reclamos, así como las acciones que resultaren pertinentes, para la protección de sus datos.
h) El titular puede manifestar la necesidad de modificar los datos que resulten ser inexactos, incompletos o inexistentes.
i) El titular de los Datos Personales puede solicitar la supresión de los mismos cuando resulten ser excesivos, no pertinentes, o el tratamiento sea contrario a las normatividad legal vigente.

AUTORIZACIÓN

Previo a la inclusión de datos personales en las bases de datos, el titular debe emitir una autorización libre, expresa e informada para su tratamiento, que podrá incluirse dentro del respectivo contrato a través del cual el titular se vincule de alguna manera con La Empresa.

No obstante, también podrán otorgarse autorizaciones independientes para el tratamiento de datos personales al que se refiere esta política.

MECANISMOS PARA OBTENER LA AUTORIZACIÓN

Los titulares de datos personales podrán emitir su autorización a través de documento físico, digitalizado por correo electrónico o por mecanismos predeterminados a través de medios técnicos.

CONSULTA

El titular, sus causahabientes o su representante y/o apoderado, pueden solicitar ante CONSTRUCTORA BERLÍN S.A.S a través del correo electrónico tramites@constructoraberlin.com o por escrito radicado en la Calle 64A # 21-50 Oficina 1701 de Manizales, Información respecto al tratamiento de los datos personales del titular, contenida en las bases de datos que maneje.

La consulta será contestada en un término máximo de 10 días hábiles contados a partir de la fecha de recibo de la misma, si no es posible atenderla en este término se le comunicará esta situación al solicitante, explicando las razones, y señalando la fecha en la que se dará respuesta, la cual no puede superar los 5 días hábiles siguientes al vencimiento del primer término.

La información que solicita el titular o sus causahabientes respecto al tratamiento de sus datos personales, podrá ser suministrada por cualquier medio, incluyendo medios electrónicos, según lo requieran, y corresponderá en todo a la que repose en la base datos.

RECLAMOS

El titular, sus causahabientes o su representante y/o apoderado que consideren que la información contenida en la base de datos debe ser objeto de corrección, los deberes para sus protección establecidos en la normatividad vigente que regula la materia, pueden presentar el reclamo correspondiente a través del correo electrónico tramites@constructoraberlin.com o por escrito radicado en la Calle 64A # 21-50 Oficina 1701 de Manizales.

DATOS SENSIBLES

LA CONSTRUCTORA BERLÍN S.A.S dentro de las actividades comerciales y constructivas que despliega no recolecta o requiere de manera habitual de datos sensibles, no obstante, cuando así se requiera, adicional a la autorización general para el tratamiento de datos personales se le informará al titular de sus datos que se hará tratamiento sobre datos de carácter sensible.

ALMACENAMIENTO DE LA INFORMACIÓN

Los datos personales objeto del tratamiento que regula esta política serán almacenados en los archivos físicos de la empresa cuando los datos sean suministrados por este medio. Por otro lado, serán almacenados en el archivo digital todos los datos que se suministren por esta vía, los cuales serán almacenados en la nube de Google Drive bajo cuentas

corporativas de la empresa, también en un *hosting* compartido de SINCOSOFT S.A.S. - SINCOSOFT S.A.S SOTFWARE BITAKORA, empresa con la cual se tiene contratado el servicio de almacenamiento de la información que pertenece a la Constructora Berlín.

Por otro lado, para el caso específico de los datos de las personas que ingresan a las obras de La Empresa, se utiliza el sistema de ingreso y salida ARHI, del cual es administrado por la encargada del tratamiento GRUPO TSM INGENIERÍA S.A.S.

En INFOLAFT - La base de datos se encuentra alojada en la plataforma de servicios de nube Amazon Web Services (AWS) y utiliza el motor de base de datos Oracle, asegurando la máxima disponibilidad, seguridad y escalamiento. El motor de búsqueda es Apache Solr, de muy alto rendimiento, escalable, potente y que tiene multitud de funcionalidades orientadas a la búsqueda permitiendo hallar variaciones cercanas por nombre y alias buscados. El sistema cuenta con un certificado SSL provisto por DigiCert, proveyendo una conexión segura para el intercambio de credenciales de acceso e información de consultas y resultados. La contraseña debe tener al menos 8 caracteres y debe contener por lo menos un carácter numérico, un carácter especial y una mayúscula, sin espacio. La contraseña distingue entre mayúsculas y minúsculas.

Para Fact-E – Dispapeles - Se incluye almacenamiento de los documentos electrónicos por un periodo de 5 años (Contados a partir del 1ero de enero del año siguiente a su generación) hasta con 2 megas en adjuntos por documento.

Al final del contrato se definirá y evaluará técnica y económicamente la operación de entrega de la información al cliente, o el borrador de esta.

Para Fact-E Los SLA dispuestos por Amazon garantizan un porcentaje de tiempo de actividad mínimo del 99,95% para Amazon EC2 y Amazon EBS dentro de una región determinada. Se recomienda que los portales sean abiertos desde el navegador google Chrome en su última versión para tener una mejor experiencia visual y de usuario. ESCALABILIDAD.

MEDIDAS DE SEGURIDAD

En el presente capítulo se establecen las medidas de seguridad, las cuales comprenden medidas técnicas, administrativas y humanas para salvaguardar la veracidad de la información, evitar su adulteración, consulta, uso o pérdida sin autorización del titular del derecho.

ACUERDOS DE CONFIDENCIALIDAD

A partir de la entrada en vigencia de la presente política de tratamiento de datos personales todo el personal vinculado con la Empresa deberá suscribir un acuerdo de confidencialidad adicional al contrato de vinculación, sin importar la naturaleza de la relación (laboral, comercial o civil). Además, todo tercero que se vincule con la empresa con posterioridad a la entrada en vigencia deberá suscribir también este acuerdo de confidencialidad, sin importar su calidad (cliente, proveedor, contratista, etc.)

MEDIDAS DE SEGURIDAD ESTRUCTURALES

La empresa cuenta con un dispositivo UTM (*Unified Threat Management)* instalado en las instalaciones de la empresa, el cual regula y controla la navegación de los equipos que se encuentren conectados en la empresa mediante políticas y controles para establecer filtros con el objetivo de proteger la seguridad informática de la empresa y de las conexiones entrantes y salientes.

INFORMACIÓN CONTENIDA EN MEDIOS FÍSICOS

Tipos de archivo físico

La empresa manejará en archivo físico todo lo que se refiere a celebración de contratos con terceros, contratación de personal, seguridad y salud en el trabajo, y aquello que versa sobre Junta Directiva, Asamblea de Accionistas y sus respectivos libros de actas y registro.

Personal encargado

La información contenida en medios físicos consta de archivos, en sentido amplio, los cuales son administrados por las siguientes áreas de personal: Trámites, Recepción, Desarrollo Humano y Organizacional y Contabilidad. Cada una de las cuales administrará aquello que les concierne de acuerdo con lo enunciado en este subcapítulo y los tipos de archivo físico descritos arriba.

Almacenamiento y seguridad de la información

Los archivos físicos serán almacenados en las oficinas de la empresa ubicadas en Calle 64 #21 – 50 de Manizales – Caldas.

Adicional a ello, la empresa cuenta con bodegas a donde es trasladada la información física que debe ser archivada y no se encuentra en uso. La destinación de cada una de las bodegas se destina para la información que versa sobre alguna de las siguientes materias: contabilidad, clientes, contratos, desarrollo humano y seguridad y salud en el trabajo.

Tanto las bodegas como los archivos físicos de las instalaciones de la empresa cuentan con su respectiva llave de acceso, la cual será administrada para cada uno de los archivos y bodegas por el área encargada de acuerdo con lo establecido en el subcapítulo “PERSONAL ENCARGADO” del título “INFORMACIÓN CONTENIDA EN MEDIOS FÍSICOS”, por tanto, en ningún caso se permitirá la libre consulta de la información.

Solicitudes de acceso a la información

Para acceder a la información que se encuentra en las oficinas de la empresa deberá solicitarse al área encargada para que esta suministre el acceso al archivo físico. No obstante, el área encargada podrá abstenerse de brindar acceso a la información si la finalidad de la consulta no es necesaria o pertinente.

En lo que respecta al acceso a la información que está almacenada en las bodegas de la empresa esta podrá ser consultada solicitando autorización al área encargada de la información, y cuando esta consulta sea autorizada, el solicitante deberá rellenar el formulario dispuesto por el área encargada donde indicará que información desea consultar.

Las autorizaciones de consulta a los que se refiere este numeral solo podrán ser realizadas por el personal vinculado con la empresa y de acuerdo a las finalidades del tratamiento de la información. En ningún caso se autorizará la consulta por parte de terceras personas a las que los titulares no hayan autorizado para realizar consultas sobre sus datos.

INFORMACIÓN CONTENIDA EN MEDIOS DIGITALES

Administración de la información y personal encargado

Conforme a lo establecido en esta política de tratamiento de datos personales, la información que contiene datos personales en formato digital se almacena en la nube de Google Drive bajo cuentas corporativas de la empresa y en un *hosting* compartido de la empresa SINCOSOFT S.A.S.

Para el caso de la nube de Google Drive cada encargado del área manejará el acceso a la información que se encuentre dentro de su equipo y dependientes. En dicho caso, solo Gerencia gozará de un *superusuario* que podrá acceder a la totalidad de la información de la empresa.

El acceso a la información almacenada en el *hosting* compartido se llevará a cabo por el (la) Director(a) de Desarrollo Humano y Organizacional de la empresa, quien será la única persona que contará con un *superusuario* que le permitirá consultar cualquier información de la empresa y permitir su consulta por los demás usuarios.

El personal encargado que se ha descrito en este numeral será quien puede crear, suprimir, conceder acceso o restringir el acceso a perfiles de cualquier personal vinculado con la empresa.

Solicitudes de acceso a la información

En tratándose de la información que reposará en la nube de Google Drive que ha contratado la empresa el encargado de cada área es la persona que podrá autorizar el acceso a la información por parte de otras áreas de la empresa.

Para el caso del *hosting* compartido al personal vinculado con la empresa se le creará un usuario mediante el cual podrá consultar la información idónea y necesaria para adelantar las labores para las que ha sido contrato o por las que se encuentra vinculado con la empresa.

Cuando algún personal solicitara el acceso a información adicional a la cual se le ha autorizado a su usuario deberá formular a través de su jefe inmediato una solicitud ya sea al encargado de la otra área de la empresa si es información de la nube, o al (la) Director(a)

de Desarrollo Humano y Organizacional para información contenida en el *hosting* compartido.

Para INFOLAFT - Los roles que permite crear la aplicación son:

• Rol de consulta: realizan consultas y conocen sus resultados, y reciben alertas de coincidencia y monitoreo de sus consultas. Todos los usuarios de consulta pueden ver todas las consultas hechas.

• Rol gestor: tienen la facultad de crear, modificar y deshabilitar usuarios en la herramienta. El administrador del sistema es el oficial de cumplimiento de la compañía. El contacto es julio.aldana@constructoraberlin.com

• Rol de alertas: reciben todas las alertas de coincidencias y monitoreo. Máximo se pueden configurar dos.

Para BITÁKORA los canales que tienen la facultad de crear, modificar y deshabilitar usuarios en la herramienta. Los administradores del sistema de la compañía son: gestionhumana@constructoraberlin.com –

La plataforma Fact-E permite definir roles de usuario los cuales definen el nivel de acceso a las diferentes funcionalidades del flujo de recepción.

- Administrador Técnico: Este usuario tiene todos los privilegios sobre el sistema. Patricia.guiceno@constructoraberlin.com
- Administrador Emisión/Recepción: Este usuario tiene privilegios para crear usuarios, asignar usuarios, crear proveedores en el módulo de Emisión y Recepción. constructoraberlinmlz@gmail.com
- Consulta Emisión/Recepción: Es un rol con acceso limitado a las opciones de emisión de facturas, solo podrá realizar consultas. Para el módulo de recepción podrá gestionar las facturas de las áreas dependiendo de los permisos con los cuente.
- Recepción: Es un rol con acceso limitado al módulo de recepción, este rol solo podrá gestionar las facturas de las áreas dependiendo de los permisos con los cuente.

Eliminación de perfiles

Es obligación del personal encargado de administrar los perfiles de acceso al *hosting* compartido de SINCOSOFT S.A.S. eliminar los perfiles del personal una vez que finalicen sus labores o ya no se encuentren vinculados con la empresa.

En igual sentido, cuando personal de la empresa que gozaba de una cuenta corporativa de Google Drive se desvincule se eliminará su perfil y se dejará trazabilidad si la información que almacenaba en la nube dicha cuenta fue eliminada o movida a otro perfil.

La eliminación de perfiles, de los sistemas diferentes a SINCOSOFT S.A.S, son administrados por los administradores de los sistemas.

Almacenamiento y seguridad de la información

Al encontrarse la información digital en un *hosting* compartido en el cual se contrató a la empresa SINCOSOFT S.A.S. se deberán atender las medidas de la política de seguridad que ha adoptado la empresa ya mencionada. Entre las medidas de seguridad con que cuentan los datos al alojarse en el *hosting* compartido se encuentran:

- Los servidores físicos se encuentran protegidos mediante una puerta metálica que requiere de una llave de acceso, la cual solo puede ser utilizada por el personal específico de SINCOSOFT S.A.S.
- Al momento de conceder acceso físico a los servidores deberá adelantarse ante SINCOSOFT S.A.S. el respectivo procedimiento de diligenciamiento de formularios y registros para ello.
- Conforme con las políticas de seguridad de SINCOSOFT S.A.S. los medios magnéticos en los cuales se encuentren copias de seguridad de los datos son almacenados por esta empresa en cajas fuertes.
- Al interior de la empresa contratada para alojar los datos no se podrán utilizar equipos de computación sino se encuentran con el debido mantenimiento y autorizados por la empresa contratada. Así mismo, no será posible utilizar y acceder a la información de la empresa mediante la utilización de medios extraíbles como discos USB y similares.
- Por otro lado, SINCOSOFT S.A.S. se ha obligado a adoptar *firewalls* y sistemas similares que garanticen que la obligación que la empresa almacena en sus servidores no pueda ser objeto de consultas por terceros no autorizados, víctima de *hacking, phishing,* virus o cualquier clase de software malicioso.

En todo caso, las medidas relatadas en el presente numeral son enunciativas, toda vez que SINCOSOFT S.A.S. actualiza y perfecciona sus medidas de seguridad respecto de la información de sus clientes, con la finalidad de evitar la fuga, alteración o pérdida de esta, incluidos los datos personales a los que se refiere este documento.

Para consultar a profundidad las medidas de seguridad podrá solicitarse la misma al correo electrónico gestionhumana@constructoraberlin.com.co

En el caso del resto de la información contenida o almacenada en la nube de Google Drive de las cuentas corporativas cada persona tendrá una clave de acceso única, la cual se ha comprometido a no revelar a terceras personas en virtud del acuerdo de confidencialidad que ha suscrito el personal al momento de vincularse con la empresa. Adicional a ello Google cuenta con todas las medidas de seguridad necesarias para que la información no pueda ser consultada por personas externas a la organización, evitando así también su adulteración, fragmentación, eliminación o uso no autorizado.

Información Referente al Ingreso y Salida de Personal en Obra

Cualquier persona que llegue a ingresar a una obra desarrollada por Constructora Berlín S.A.S. deberá registrarse en el sistema de ingreso y salida denominado ARHI, que es administrado por la encargada del tratamiento de datos GRUPO TSM INGENIERÍA S.A.S.

Información Referente al sistema de consultas INFOLAFT SAGRILAFT

Infolaft Search es un servicio por medio del cual se provee la consulta consolidada de listas, provenientes de fuentes de información relacionadas con los riesgos de lavado de activos, financiación del terrorismo, corrupción, fraude y reputacional permitiéndole identificar el riesgo asociado de sus contrapartes.

- Acceso a través de un navegador de internet estándar, sin necesidad de instalar aplicaciones mediante licenciamiento SaaS (Software As A Service).
- Las consultas se pueden realizar por medio del nombre y/o número de identificación y de forma individual o masiva, mediante la carga de un archivo de Excel.
- Cuenta con tres sistemas de alertas: búsqueda ya realizada, por coincidencia y por monitoreo.
- Clasificación de las coincidencias encontradas en escalas y organizando las coincidencias encontradas según su riesgo asociado y su diferencia con el valor buscado.
- Almacenamiento de los reportes de resultados hechos por todos los usuarios (de forma individual o masiva) y la posibilidad de exportarlos en formatos PDF, Excel o texto. Los reportes incluyen toda la información provista por cada una de las listas sobre las coincidencias encontradas e información sobre la fecha, hora y usuario de búsqueda.
- Reportes especializados para descartar homónimos y funciones específicas para hacer eficiente la consulta en listas restrictivas.
- Plena observancia del derecho de autor protección de datos determinados por la ley colombiana y las particularidades de cada una.
- El sistema alerta cuando una búsqueda haya sido previamente hecha, evitando dobles consumos.
- El sistema alerta cuando una consulta hecha durante los últimos 12 meses (contados desde la fecha de la consulta) cambia la cantidad de coincidencias en las que aparecía originalmente, permitiendo un control de riesgo oportuno.
- La alerta se evidencia mediante el envío de un correo electrónico dirigido a la persona que realizó la consulta original y al usuario administrador, adjuntando el informe actualizado de resultados dentro del correo electrónico como un archivo adjunto.

Información Referente al sistema de Consultoria para implementación del SOFTWARE – BITAKORA.

EL PRESTADOR prestara servicio de arrendamiento de licencia de uso no exclusivo del software BITÁKORA para el manejo de: NÓMINA: Liquidación de Nómina, Nómina Electrónica, Portal Empleados.
BITAKORA cuenta con la integración automatizada de nómina electrónica con el operador tecnológico autorizado: SAPHETY bajo un esquema integrado que permite emitir documentos soporte y notas de ajuste electrónicas en los procesos generados desde BITÁKORA.

Información colaboración electrónica ecosistema de soluciones – DISPAPELES SAS Fact-2.

Fact-e de Dispapeles expone a sus clientes una solución integrada a la herramienta Fact-e, a fin de mejorar los procesos de recepción de facturas, cuentas por pagar, facturas rechazadas y aprobaciones de pago.

El módulo de recepción en la plataforma de Fact-e, en esta plataforma se encuentra automatizado el proceso de recepción de facturas electrónicas las cuales se leen a través de un correo de recepción previamente configurado y como complemento para las facturas no electrónicas contamos con la plataforma Fact-E Adquirientes y Proveedores en las cuales los proveedores no electrónicos podrán cargar su facturación llegando a una única plataforma con toda la facturación.

Módulo de recepción para facturas electrónicas y no electrónicas configura sus facturas, notas débito y notas Crédito, portal de proveedores para consulta de documentos emitidos.

El portal Fact-e cuenta con la opción de notificar a cada usuario que este asociado a las determinadas áreas del flujo de recepción asegurando de esta manera que el usuario tenga conocimiento de sus nuevas facturas pendientes y de la misma manera asegurar que el proceso no se detenga. Cada factura cuenta con su historial y su historio de gestiones para garantizar la transparencia y trazabilidad en cada interacción de las facturas.

Recepción de documentos electrónicos y no electrónicos a través del portal con integración al ERP.

Este flujo cuanta con 1 área, 3 tareas y 2 acciones, los títulos de las diferentes cajas se pueden modificar teniendo en cuenta que no pueden exceder el número de caracteres por área (45), tareas (45), descripción (200) y acciones (45).

Información SAPHETY transacciones electrónicas S.A.S

Se presta el servicio de Facturacion electrónica a través del uso de la plataforma SaphetyDoc, la generación y emisión de transacciones en formato electrónico, a partir de la información enviada por el cliente y atreves de la API suministrada por SAPHETY; al efecto y que necesita ser acreditada y configurada por el cliente. Así mismo permitir al cliente a través de la plataforma la generación y emisión de nóminas en formato electrónico, bien sea como notas crédito y/o como notas débito, desde cualquier sistema de gestión

(ERP o CRM); por medio de comunicaciones vía API de archivos en formato JSON, permitiendo así cumplir con las exigencias establecidas por la Dian de forma automatizada. Bajo el siguiente esquema:

- Generación desde el Software de nómina =) entrega a Saphety =) Envió y reporte a la DIAN y validación =) Entrega al empleado.

Medidas de Seguridad de los sistemas

El sistema ARHI será utilizado para consignar datos de las personas que ingresan a las obras de la Empresa como se expresó en el acápite anterior. No obstante, a través del sistema solo se obtiene la información con la administración de la encargada del tratamiento y dicha información posteriormente es almacenada bajo las mismas condiciones y seguridades de la información contenida en medios digitales a las que se refiere este capítulo, más precisamente se hace un intercambio de información a través de la nube de Google Drive y de esta manera la Encargada del tratamiento de datos transmite los mismos al Responsable.

En todo caso, lo anterior no implica que con la encargada del tratamiento de datos que administra la información que transita a través del sistema ARHI no se hayan celebrados los respectivos acuerdos contractuales y de confidencialidad para asegurar el cumplimiento de las obligaciones contenidas en esta política.

Asimismo, GRUPO TSM INGENIERÍA S.A.S. garantiza a la Empresa que ha adoptado todas las medidas necesarias para garantizar la seguridad de la información en lo que respecta a su encargo en el tratamiento de datos, por lo que ante cualquier duda sobre este procedimiento podrán enviarse consultas a la dirección gestionhumana@constructoraberlin.com.co

Para INFOLAFT - Las Partes tomarán todas las medidas pertinentes para garantizar la seguridad de la Información Confidencial y evitar la pérdida, acceso o modificación de la misma por personas no autorizadas. En este sentido, la Parte Receptora se compromete a mantener restringido el acceso a los equipos de cómputo en los cuales se almacene Información Confidencial y a asignar contraseñas seguras, así como a implementar y tomar todas las medidas y acciones necesarias para garantizar la custodia y conservación de la Información Confidencial, cualquiera sea su medio de conservación.

Las Partes se abstendrán en lo sucesivo de efectuar para sí o para terceros, copias, arreglos, reproducciones, adaptaciones o cualquier otra clase de mutilación, deformación o modificación de la Información Confidencial. No obstante, la Parte Receptora podrá hacer copias de la Información Confidencial para suministrarla a aquellos empleados, funcionarios, asesores y consultores autorizados para ello.

Para Fact-e, Dispapeles - Los servicios IAAS ofrecen una disponibilidad del servicio por encima del 99%, esto gracias a que la infraestructura de sus Data Center es redundante, y están plenamente certificados, cuentan con calificación de TIER nivel 4.

En todo momento se tiene el control de la instancia, por lo tanto, estas pueden ser iniciadas, reiniciadas o detenidas cuando sea necesario. Todo esto de manera remota, pero con un control total como si fuese un pc personal.

SAPHETY se compromete a asegurar, de conformidad con lo establecido en el acuerdo de los niveles de servicio y salvo en los casos de fuerza mayor, caso fortuito o hechos relacionados con la culpa o dolo del cliente, las condiciones tecnológicas necesarias para el correcto funcionamiento de la plataforma SaphetyDoc. Saphety se compromete a asegurar, de conformidad con lo establecido en el acuerdo de niveles de servicio, las condiciones tecnológicas necesarias para el correcto funcionamiento de la plataforma.

DATOS SENSIBLES

En el evento en que se recolecten datos de carácter sensible, se sujetarán a las mismas medidas de seguridad. Sin embargo, salvo que sea indispensable para el cumplimiento de los fines y funciones de la empresa, se procurará que los datos de esta naturaleza sean consultados lo mínimo posible aun cuando sea solicitado por personal de la misma empresa, de manera que estos datos conserven toda la confidencialidad de su naturaleza.

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES

Cuando se presente algún incidente que pueda poner en riesgo la seguridad de los datos personales o que se pueda consultar por personas no autorizadas, deberá aplicarse el protocolo de gestión de incidentes contenido en este acápite, sin importar que se trate de datos contenidos en medios físicos, digitales

Notificación del Incidente

Cuando ocurra algún incidente relacionado con los datos personales sobre los cuales se realiza el tratamiento por parte de la empresa, el personal encargado al interior de la entidad deberá de informar esta situación a su superior jerárquico al interior de la empresa para que se inicien la investigación y las eventuales medidas correctivas del caso.

Similar aviso deberá darse a SINCOSOFT S.A.S. o GRUPO TSM INGENIERÍA S.A.S. para que despliegue el procedimiento de incidentes que contiene su política de seguridad cuando se evidencie que el incidente puede tener implicaciones de o para tal empresa.

Soporte Documental

El personal encargado para cada base de datos al evidenciar algún incidente en los mismos deberá dejar el soporte documental necesario en el cual deberá indicar: descripción del incidente, categoría de datos personales en riesgo (públicos, semiprivados, sensibles, etc.), la fecha y hora en qué se conoció el incidente o en la que inicio el mismo, la conclusiones preliminares y si se han adoptado medidas correctivas de manera provisional para evitar el aumento del riesgo, si existe otro personal que tenga alguna relación con el incidente ocurrido, la evaluación del nivel de riesgo del incidente, la constancia de haberse notificado a la Superintendencia de Industria y Comercio como autoridad de datos personales o que se hará dentro del término establecido, la constancia de notificación a los titulares de los

datos personales cuando fuera necesario, y la inclusión de otros detalles necesarios para conocimiento del incidente.

Informe a la Superintendencia de Industria y Comercio

Dentro de los 15 días hábiles siguientes al momento de detectarse el incidente, el Encargado del tratamiento de los datos personales deberá elevar el reporte del incidente a la Superintendencia de Industria y Comercio como autoridad nacional en materia de protección de datos personales, haciendo uso de los links dispuestos por la entidad en su página web.

Investigación del Incidente y Medidas Correctivas

El Encargado del tratamiento de datos personales deberá abrir una investigación interna para establecer cuál fue la posible causa del incidente y adoptar las medidas correctivas a que haya lugar para evitar futuros incidentes relacionados con las mismas causas.
Será necesario notificar a la Superintendencia de Industria y Comercio o a los titulares de los datos personales cuando se evidencia necesario de acuerdo con los principios y deberes de la presente política, así como lo dispuesto en las normas que regulan la materia.

Cierre del Incidente

Después de haberse cumplido todos los pasos para el manejo del incidente de datos personales el Encargado dejará el respectivo soporte documental con el análisis del caso, su causa y las medidas correctivas adoptadas.

DESTRUCCIÓN DE LA INFORMACIÓN

Cuando se destruya información contenida en medios físicos, o digitales deberá realizarse mediante procedimientos que no permitan su reconstrucción por ninguna persona.

Igualmente, cuando se lleva a cabo una destrucción de la información deberá dejarse constancia documental de la acción que se adelantó y los funcionarios vinculados a esta acción.

Para INFOLAFT a petición de la Parte Reveladora, la Parte Receptora deberá devolver todos los originales, copias, reproducciones y resúmenes de Información Confidencial, o deberá certificar la destrucción de dicha Información Confidencial.

VIGENCIA

Este manual entra en vigencia a partir de su publicación.

Manizales, Febrero 06 de 2023.