POLÍTICA DE TRATAMIENTO DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD IMPERIO LTDA

De conformidad con los lineamientos señalados en la ley 1581 de 2012, como marco de referencia legal en la implementación del manual interno de política y procedimiento para garantizar el adecuado cumplimiento de la ley, según lo ordenado en el literal K, del artículo 17 ibídem, se procede a establecer lo anterior de conformidad con el señalamiento normativo aplicable.

Dando alcance al objeto de la norma rectora respecto al derecho constitucional a conocer, actualizar y rectificar la información que se tenga sobre las personas que mantienen relación directa con **SEGURIDAD IMPERIO LTDA.**, mediante bases de datos o archivos, la política interna a implementar no puede ser disonante de la contenida en la ley estatutaria que aquí nos rige, por ello los principios rectores contemplados en el título II, se erigen como el elemento fundamental para el manejo, protección, suministro y guarda de la información.

IDENTIFICACIÓN, NOMBRE Y OBJETO SOCIAL DE LA EMPRESA

SEGURIDAD IMPERIO LTDA identificada con Nit 830.080.581-0 empresa legalmente constituida cuyo objeto principal se encuentra enmarcado en las siguientes actividades: La prestación remunerada de servicios de vigilancia y seguridad privada, en la modalidad de vigilancia fija y móvil y/o escolta a personas, a mercancías con y sin armas de fuego y medios tecnológicos.

ALCANCE

Esta Política de Tratamiento y seguridad de la Información se aplicará a todas las Bases de Datos y/o Archivos que contengan Datos Personales que sean objeto de Tratamiento por parte de SEGURIDAD IMPERIO LTDA, considerada como responsable y/o encargada del tratamiento de Datos Personales.

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

SEGURIDAD IMPERIO LTDA, CON NIT 830.080.581-0, con domicilio en la Cra 27 C No. 71 B 45 de la ciudad de Bogotá D.C., Colombia. Correo electrónico: protecciondedatos@seguridadimperio.com.co tel. 7424954.

MARCO LEGAL

Constitución Política, artículo 15.

Ley 1266 de 2008 Reglamentada parcialmente por el Decreto 2952 de 2010 en sus artículos 12 y 13 y el Decreto 1727 de 2009 reglamentaria de su artículo 14.

Ley 1581 de 2012 Reglamentada Parcialmente por el Decreto 1377 de 2013 y el Decreto 886 de 2014

DEFINICIONES

Conforme a lo dispuesto en el artículo 3 de la Ley 1581 de 2012 ***"Por la cual se dictan disposiciones generales para la protección de datos personales."*** **Que tiene por "***objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."* Y su Decreto Reglamentario se establece como definiciones en el desarrollo de la Ley las siguientes:

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 y seguridad de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

BASE DE DATOS: conjunto organizado de datos personales que sea objeto de tratamiento.

CAUSAHABIENTE: persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

DATO PERSONAL: cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse a una persona natural o jurídica.

DATO PÚBLICO: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

DATOS SENSIBLES: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos

que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

DATOS OPCIONALES: son aquellos datos que la EMPRESA requiere para ofrecer servicios adicionales.

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.

LEY DE PROTECCIÓN DE DATOS: es la Ley 1581 de 2012 y sus Decretos reglamentarios o las normas que los modifiquen, complementen o sustituyan.

HABEAS DATA: derecho de cualquier persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.

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 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 la recolección, almacenamiento, uso, circulación o supresión
.
TRANSFERENCIA: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

TRANSMISIÓN: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

TRATAMIENTO

SEGURIDAD IMPERIO LTDA, actuando en calidad de Responsable del Tratamiento de Datos Personales, para el adecuado desarrollo de sus actividades comerciales, así como para el fortalecimiento de sus relaciones con terceros, recolecta, almacena, usa, circula y suprime Datos Personales correspondientes a personas naturales con quienes tiene o ha tenido relación, sin que la enumeración signifique limitación, trabajadores y familiares de éstos, clientes, proveedores, acreedores, deudores y visitantes.

PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

En el desarrollo, interpretación y aplicación de la ley 1581 de 2012, se aplicarán de manera armónica e integral los siguientes principios rectores contemplados en la misma, así:

"a) PRINCIPIO DE LA LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS: El Tratamiento de datos a que se refiere la Ley que nos ocupa es una actividad reglada que debe sujetarse a lo estableció en la ley y las demás disposiciones que la desarrollen.

b) PRINCIPIO DE FINALIDAD: el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, que debe ser informada al titular.

c) PRINCIPIO DE LIBERTAD: el tratamiento solo puede ejercerse con el consentimiento previo, expreso, e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) PRINCIPIO DE VERACIDAD O CALIDAD: la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) PRINCIPIO DE TRANSPARENCIA: en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA: el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.

g) PRINCIPIO DE SEGURIDAD: la información sujeta a tratamiento por la EMPRESA se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) PRINCIPIO DE CONFIDENCIALIDAD: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Las personas cuyos Datos Personales sean objeto de Tratamiento por parte de **SEGURIDAD IMPERIO LTDA**, tienen los siguientes derechos, los cuales pueden ejercer en cualquier momento:

a) Conocer, actualizar y rectificar sus datos personales frente a **SEGURIDAD IMPERIO LTDA**, en su condición de Responsable del Tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada a **SEGURIDAD IMPERIO LTDA** salvo cuando expresamente se exceptúe como requisito para el tratamiento (casos en los cuales no es necesaria la autorización) de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012

c) Ser informado por **SEGURIDAD IMPERIO LTDA**, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que la EMPRESA ha incurrido en conductas contrarias a la ley que nos ocupa y a la Constitución

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

AUTORIZACIONES Y CONSENTIMIENTO DEL TITULAR

El artículo 9 de la Ley 1581 de 2012 señaló:
"Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior."
A su vez el artículo 5 del Decreto 1377 de 2013 reglamentario de la Ley 1581 de 2012 señaló:

"El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. /// Los datos personales que se encuentren en fuentes de acceso

público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos. /// En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este decreto, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el Responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento."

El artículo 6 ibídem respecto a los datos personales sensibles dispuso:
"De la autorización para el Tratamiento de datos personales sensibles*.* El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. /// En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

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

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

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles."

MEDIO Y MANIFESTACIÓN PARA OTORGAR LA AUTORIZACIÓN DEL TITULAR

SEGURIDAD IMPERIO LTDA en cumplimiento a lo dispuesto en la Ley, instruyó a las personas encargas de la recolección y trámite de datos personales para que este trámite se limite a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos, para lo anterior implementó las autorizaciones escritas de los titulares.

EVENTOS EN LOS CUALES NO ES NECESARIA LA AUTORIZACIÓN DEL TITULAR DE LOS DATOS PERSONALES

La autorización del titular de la información no será necesaria en los siguientes casos:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b) Datos de naturaleza pública.

c) Casos de urgencia médica o sanitaria.

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. Datos relacionados con el Registro Civil de las personas.

TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS Y FINALIDAD DEL MISMO

El tratamiento para los datos personales indispensables estará enmarcado en el orden legal y serán todos los necesarios para el cumplimiento de la misión institucional. Para el caso de datos personales sensibles, se podrá hacer uso y tratamiento de ellos cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y/o requisitos:

a) que respondan y respeten el interés superior de los niños, niñas y adolescentes.

b) que se asegure el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. La EMPRESA velará por el uso adecuado del tratamiento de los datos personales de los niños, niñas o adolescentes.

PERSONAS A QUIENES SE LES PUEDE SUMINISTRAR LA INFORMACIÓN

La información que reúna las condiciones establecidas en la ley podrá suministrarse a las siguientes personas:

a) A los titulares, sus causahabientes (cuando aquellos falten) o sus representantes legales.

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

c) A los terceros autorizados por el titular o por la ley.

LIMITACIONES TEMPORALES AL TRATAMIENTO DE LOS DATOS PERSONALES.

LA EMPRESA solo podrá recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida finalidad del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, procederá a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual

LEGITIMACIÓN PARA EL EJERCICIO DEL DERECHO DEL TITULAR

Los derechos de los titulares establecidos en Decreto Reglamentario 1377 de 2013 artículo 20 podrán ejercerse por las siguientes personas:

"a) Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición **SEGURIDAD IMPERIO LTDA**

b) Por los causahabientes del titular, quienes deberán acreditar tal calidad.

c) Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.

d) Por estipulación a favor de otro o para otro.
Los derechos de los niños, niñas y adolescentes se ejercerán por las personas que estén facultadas para representarlos."

ÁREA RESPONSABLE DE LA IMPLEMENTACIÓN Y OBSERVANCIA DE ESTA POLÍTICA

EL JEFE DE MEDIOS TECNOLÓGICOS DE SEGURIDAD IMPERIO LTDA, tiene a su cargo la labor de desarrollo, implementación, capacitación y observancia de ésta Política.

EL JEFE DE INVESTIGACIONES Y ATENCIÓN AL USUARIO, también ha sido designado por SEGURIDAD IMPERIO LTDA como área responsable de la atención de peticiones, consultas, quejas y reclamos ante la cual el Titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

DEBERES DE LA EMPRESA

En virtud de la presente política de tratamiento y protección de datos personales son deberes de SEGURIDAD IMPERIO LTDA, sin perjuicio de las demás disposiciones previstas en la ley 1581 de 2012 y en sus Decretos Reglamentarios, los siguientes,

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 en virtud de la autorización otorgada.

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

e) Garantizar que la información suministrada sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente.

h) Respetar las condiciones de seguridad y privacidad de la información del titular.

i) Tramitar las consultas y reclamos formulados en los términos señalados por la ley.

j) Identificar cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

k) Informar a solicitud del titular sobre el uso dado a sus datos.

l) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

m) Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.

n) Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 de 2012.

o) **SEGURIDAD IMPERIO LTDA** hará uso de los datos personales del titular solo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales.

DISPOSICIONES ESPECIALES PARA EL TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES

Según lo dispuesto por el Artículo 7º de la Ley 1581 de 2012 y el artículo 12 del Decreto 1377 de 2013, SEGURIDAD IMPERIO LTDA sólo realizará el Tratamiento, esto es, la recolección, almacenamiento, uso, circulación y/o supresión de Datos Personales correspondientes a niños, niñas y adolescentes, siempre y cuando este Tratamiento responda y respete el interés superior de los niños, niñas y adolescentes y asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, **SEGURIDAD IMPERIO LTDA** deberá obtener la Autorización del representante legal del niño, niña o adolescente, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

PROCEDIMIENTO PARA ATENCIÓN Y RESPUESTA A PETICIONES, CONSULTAS, QUEJAS Y RECLAMOS DE LOS TITULARES DE DATOS PERSONALES

a) **CONSULTAS**: Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en SEGURIDAD IMPERIO LTDA quien suministrará toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. La consulta se formulará a través del correo protecciondedatos@seguridadimperio.com.co y será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

b) **RECLAMOS**: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante la EMPRESA el cual será tramitado bajo las siguientes reglas:

1. El reclamo del Titular se formulará mediante solicitud dirigida a SEGURIDAD IMPERIO LTDA a través del correo electrónico protecciondedatos@seguridadimperio.com.co con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo en el correo protecciondedatos@seguridadimperio.com.co, éste se catalogará con la etiqueta "RECLAMO EN TRÁMITE" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha etiqueta se mantendrá hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

c) **PETICIÓN DE ACTUALIZACIÓN, RECTIFICACIÓN Y SUPRESIÓN DE DATOS**. SEGURIDAD IMPERIO LTDA rectificará y actualizará, a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual el titular allegará la solicitud al correo electrónico protecciondedatos@seguridadimperio.com.co indicando la actualización, rectificación y supresión del dato y aportará la documentación que soporte su petición.

d) **REVOCATORIA DE LA AUTORIZACIÓN Y/O SUPRESIÓN DEL DATO LOS TITULARES DE LOS DATOS PERSONALES**. Pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual, para ello SEGURIDAD IMPERIO LTDA pondrá a disposición del Titular el correo electrónico protecciondedatos@seguridadimperio.com.co. Si vencido el término legal respectivo, SEGURIDAD IMPERIO LTDA, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

SEGURIDAD DE LOS DATOS PERSONALES

El propósito de la siguiente política es fijar las directrices encaminadas a proteger los datos privados y confidenciales de nuestra empresa, de nuestros empleados y de nuestros clientes, así mismo asegurar que se utilicen correctamente los recursos tecnológicos que la empresa pone a disposición de sus empleados para el desarrollo de sus funciones.

La información incluye datos mantenidos en los sistemas de **SEGURIDAD IMPERIO LTDA**, en soporte físico (papel), correos electrónicos, registros de llamadas, memorias USB, discos duros y compactos, dispositivos móviles u otros medios de almacenamiento. El tratamiento apropiado de los datos personales es fundamental para ganarse la confianza tanto de nuestros clientes como de nuestros colaboradores.

Esta política es de obligatorio cumplimiento. El funcionario que la incumpla, responderá por sus acciones, omisiones o por los daños causados a la infraestructura de información de la empresa, de conformidad con la normatividad penal vigente y la disciplinaria de la empresa.

Es obligación de todos los empleados atender las siguientes directrices:

CUENTAS DE USUARIOS

- Cada persona que acceda a su equipo de cómputo y al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control y evita que interfieran las configuraciones de distintos usuarios.
- El Jefe de Medios Tecnológicos es el único usuario administrador de cada equipo de cómputo y del sistema. En caso de ausencia, la Gerencia General deberá tener acceso a la contraseña de usuario administrador y designar a quien considere competente para atender algún requerimiento de mantenimiento.
- La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito y ser debidamente autorizada por el Jefe de Medios Tecnológicos.
- Cuando un usuario recibe una cuenta, debe firmar este documento donde declara conocer las políticas de tratamiento de datos y procedimientos de seguridad de la información y acepta sus responsabilidades con relación al uso de su cuenta.
- No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Gerencia General.
- Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye al usuario administrador del sistema.
- Los Directores de cada área deben reportar al Jefe de Medios Tecnológicos sobre los empleados bajo su encargo que cesan sus actividades y solicitar la desactivación de su cuenta.

- No se otorgará cuentas a técnicos de mantenimiento externos, ni se permitirá su acceso remoto, a menos que el responsable de los sistemas de información determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- No se crearán cuentas anónimas o de invitado.

INTERNET

Internet es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas para poder acceder a la información de la empresa.

- El acceso a internet es únicamente de uso laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.
- Está prohibido acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.
- En ningún caso se puede recibir ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.
- Se prohíbe descargar programas, demos, tutoriales, ficheros o documentos que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado y que contravengan las normas de Seguridad Imperio Ltda. sobre instalación de software y propiedad intelectual.
- Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo al Jefe de Medios Tecnológicos quien determinará su conveniencia y cotizará a través del proceso de compras, previa autorización de la Gerencia General.
- Está prohibido instalar programas para ver vídeos, emisoras de televisión y de música vía Internet (ARES, REAL AUDIO, BWV, etc.).
- No debe usarse el Internet para realizar llamadas internacionales (Dialpad, Skype, NET2PHONE, FREEPHONE, etc.)
- Los empleados tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

CORREO ELECTRÓNICO

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones que apoyen la gestión de la empresa en el desarrollo de su objeto social.

Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.

Es obligación del empleado:

- Utilizar el correo electrónico como una herramienta de trabajo, y no como casilla personal de mensajes, para eso está el correo particular.
- Evitar enviar archivos de gran tamaño a compañeros de oficina. Si se hace necesario compartir un archivo con estas características deberá publicarlo en la red.
- Evitar participar en la propagación de mensajes encadenados o en esquemas piramidales o similares.
- Evitar distribuir mensajes con contenidos impropios y/o lesivos a la moral.
- Si se recibe un correo de origen desconocido, debe consultar inmediatamente con el Coordinador de Medios Tecnológicos sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).
- Evitar poner "Contestar a todos" cuando se contesta un correo a no ser que este absolutamente seguro que el mensaje puede ser recibido por todos los intervinientes. De igual forma si va a reenviar un correo.
- Evitar el acceso a las cuentas personales durante la jornada laboral.
- Cerrar el software de correo electrónico cuando deje de usar su estación de trabajo para evitar que otra persona use su cuenta de correo.
- Se prohíbe facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.
- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje. Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- Enviar mensajes bien formateados y evitar como norma de cortesía, el uso generalizado de letras mayúsculas.

- Evitar usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
- Evitar enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- El Jefe de Medios Tecnológicos determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.
- Los mensajes tendrán una vigencia no mayor de 30 días desde la fecha de entrega o recepción de los mismos. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo.
- Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales en el disco duro del computador personal.

COMPUTADORES, IMPRESORAS, PERIFÉRICOS Y LÍNEAS TELEFÓNICAS FIJAS Y MÓVILES

- La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.
- Está prohibido el uso de líneas telefónicas fijas y móviles para comunicación distinta a la relacionada con el trabajo.
- Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador. Es competencia del Coordinador de Medios Tecnológicos la instalación de software.
- No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia del Coordinador de Medios Tecnológicos, el retiro o cambio de partes.
- Cualquier medio externo de almacenamiento de información traído a la empresa, debe superar una verificación de virus mediante el antivirus instalado, en su defecto, debe ser entregado al Coordinador de Medios Tecnológicos para control de circulación de virus.
- No es permitido destapar o retirar la tapa de los equipos, por personal diferente al Coordinador de Medios Tecnológicos o bien a quien designe sin la autorización de este.
- Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización del Coordinador de Medios Tecnológicos.
- Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.
- Es estrictamente obligatorio, informar oportunamente al Coordinador de Medios Tecnológicos la ocurrencia de novedades por problemas técnicos, eléctricos, de

planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse tan pronto se presente el problema.

- Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.
- Los protectores de pantalla y tapiz de escritorio, serán establecidos por Coordinador de Medios Tecnológicos y deben ser homogéneos para todos los usuarios.
- Ningún empleado, podrá formatear los discos duros de los computadores.
- Ningún empleado podrá retirar o implementar partes sin la autorización de la Oficina de sistemas.

OTRAS POLÍTICAS

- La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar sin la autorización del Coordinador de Medios Tecnológicos porque esto ocasionaría conflictos de IP'S y esto alteraría el flujo de la red.
- No llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.
- Todo empleado responsable de equipos informáticos debe dejarlo en modo de hibernación al medio día y apagado en la noche lo anterior para ahorrar recursos energéticos y contribuir a la conservación de los equipos.

Archivo físico y documentos

• Cada Líder de Proceso es responsable por el archivo de sus registros tanto físicos como electrónicos haciéndolo de tal manera que permita una oportuna ubicación y trazabilidad. Así mismo se hace responsable de salvaguardar los intereses de la compañía, dando la debida protección a información que se considere sensible.

• Se considera justa causa para la terminación unilateral del contrato de trabajo, sin perjuicio de las acciones penales que puedan derivar de la acción, quien brinde información de la compañía a terceros sin la debida autorización y cuyo uso pueda ser perjudicial para la labor comercial de la compañía y su competitividad en el mercado.

• Con el ánimo de prevenir fraudes, no se firmarán contratos laborales o comerciales por parte del representante legal o quien haga sus veces, hasta tanto sean debidamente validados.

• La información laboral contenida en las hojas de vida de los empleados tiene carácter de confidencial por lo tanto no podrá exhibirse a personas diferentes al representante legal o la autoridad requirente.

Correspondencia:

• Los documentos producidos en la empresa tienen un funcionario quien los emite, quien es el responsable de controlar su envío a la persona o entidad destinataria, el recibo por parte del destinatario, así como de controlar la llegada, trámite y archivo de la copia con el respectivo sello de recibido.

• Los documentos llegados a la empresa, tienen un destinatario específico, quien es el responsable de recibirlo, darle el trámite correspondiente, controlar que produzca los efectos requeridos y su posterior archivo.

• Para los efectos anteriores, se disponen de dos libros de correspondencia separados denominados Libro de Correspondencia Salida y Libro de Correspondencia Llegada.

• Todo funcionario que elabore un documento, debe responsabilizarse del control y seguimiento del mismo hasta que finalice el proceso correspondiente, así como de su archivo y conservación para consultas.

POLÍTICAS DE SEGURIDAD EN SERVIDOR

Se implementara un servidor bien sea físico o en la nube con las siguientes características en su software de desarrollo:

- Debe existir un reporte de trazabilidad de los usuarios que ingresan, modifican y extraen información de los servidores.
- Cada usuario deberá tener una carpeta debidamente organizada para que la información a resguardar sea de fácil acceso y ubicación.
- El coordinador de medios tecnológico estará encargado de asignar cada una de las carpetas y asignar a cada usuario su clave de acceso y asignara los permisos necesarios para que otros usuarios tengan acceso a información de diferentes usuarios

"El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de sus empleados".

SEGURIDAD IMPERIO LTDA tras implementar la política de seguridad de los datos, no garantiza la seguridad total de su información ni se responsabiliza por cualquier consecuencia derivada de fallas técnicas o del ingreso indebido por parte de terceros a la Base de Datos o Archivo en los que reposan los Datos Personales objeto de Tratamiento por parte de LA EMPRESA y sus Encargados.

TRANSFERENCIA, TRANSMISIÓN Y REVELACIÓN DE DATOS PERSONALES

SEGURIDAD IMPERIO LTDA podrá revelar los Datos Personales sobre los cuales realiza el Tratamiento, para su utilización y Tratamiento conforme a esta Política de Protección de Datos Personales.

Igualmente, podrá entregar los Datos Personales a terceros no vinculados cuando: a.) Se trate de contratistas en ejecución de contratos para el desarrollo de sus

actividades; b.) Por transferencia a cualquier título de cualquier línea de negocio con la que se relaciona la información.

En todo caso, en los contratos de transmisión de Datos Personales, que se suscriban entre **SEGURIDAD IMPERIO LTDA** y los Encargados para el Tratamiento de Datos Personales, se exigirá que la información sea tratada conforme a esta Política de Protección de Datos Personales y se incluirán las siguientes obligaciones en cabeza del respectivo Encargado:

Dar Tratamiento, a nombre de **SEGURIDAD IMPERIO LTDA** a los Datos Personales conforme los principios que los tutelan.
Salvaguardar la seguridad de las bases de datos en los que se contengan Datos Personales.
Guardar confidencialidad respecto del Tratamiento de los Datos Personales.

TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES

SEGURIDAD IMPERIO LTDA en cumplimiento a lo dispuesto en la ley y en consideración de sus vínculos permanentes u ocasionales de carácter comercial con empresas internacionales, podrá efectuar transferencia y transmisión de datos personales de los titulares.

Para la transferencia internacionales de datos personales de los titulares, SEGURIDAD IMPERIO LTDA tomará las medidas necesarias para que los terceros conozcan y se comprometan a observar esta Política, bajo el entendido que la información personal que reciban, únicamente podrán ser utilizada para asuntos directamente relacionados con **SEGURIDAD IMPERIO LTDA** y solamente mientras ésta dure y no podrá ser usada o destinada para propósito o fin diferente.

Para la transferencia internacional de datos personales se observará lo previsto en el artículo 26 de la Ley 1581 de 2012. Las transmisiones internacionales de datos personales que efectúe **SEGURIDAD IMPERIO LTDA** no requerirán ser informadas al Titular ni contar con su consentimiento cuando medie un contrato de transmisión de datos personales de conformidad al artículo 25 del Decreto 1377 de 2013.

DATOS RECOLECTADOS ANTES DE LA EXPEDICIÓN DEL DECRETO 1377 DE 2013

De conformidad con lo dispuesto en el numeral 3 del artículo 10 del Decreto Reglamentario 1377 de 2013 SEGURIDAD IMPERIO LTDA procederá a publicar un aviso en su página web oficial www.seguridadimperio.com.co dirigido a los titulares de datos personales para efectos de dar a conocer la presente política de tratamiento de información y el modo de ejercer sus derechos como titulares de datos personales alojados en sus bases de datos.

MEDIDAS DE SEGURIDAD

En desarrollo del principio de seguridad establecido en la Ley 1581 de 2012, **SEGURIDAD IMPERIO LTDA** adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El personal que realice el tratamiento de los datos personales ejecutará los protocolos establecidos con el fin de garantizar la seguridad de la información.

FECHA DE ENTRADA EN VIGENCIA

La presente Política de Datos Personales fue creada el día 5 de septiembre de 2016 y entra en vigencia a partir del día 1 de octubre 2016. Cualquier cambio que se presente respecto de la misma, se informará a través de página web www.seguridadimperio.com.co

"El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de los empleados de Seguridad Imperio Ltda".

_____

Gerente General Bogotá D.C.,
Septiembre 5 de 2016