CONTENIDO

I. GENERALIDADES – APLICACIÓN – DEFINICIONES – PRINCIPIOS

La Ley 1581 de 2012, por medio de la cual se dictan disposiciones generales para la protección de datos personales en Colombia, y el Decreto Nacional 1377 de 2013, por medio del cual se reglamenta parcialmente la Ley 1581 de 2012, tienen aplicación a los datos personales que se encuentren registrados o depositados en cualquier base de datos que los haga susceptible de Tratamiento.

INFOTIC S.A., como Responsable y/o Encargado del Tratamiento de datos personales, utilizará este Manual para el Tratamiento de Datos Personales para fijar los principios y bases fundamentales sobre las cuales se llevará a cabo el Tratamiento de datos personales que realice en el desarrollo de su objeto social.

El presente Lineamiento está destinado a aplicarse al Tratamiento de datos personales que no se encuentren excluidos de modo expreso por la Ley. Se excluyen de la aplicación de la Ley:

a. Bases de datos mantenidas en ámbitos exclusivamente personales o domésticos (siempre que no vayan a ser suministradas a terceros, caso en el cual, se deberá informar y solicitar autorización del Titular).
b. Bases de datos y archivos relacionados con seguridad y defensa nacional, así como la prevención, detección y monitoreo de lavado de activos o actividades de financiación del terrorismo.
c. Bases de datos que contengan información de inteligencia y contrainteligencia.
d. Bases de datos y archivos de información periodística y otros contenidos editoriales.
e. Bases de datos y archivos regulados por el régimen de hábeas data financiero y crediticio.
f. Bases de datos relacionadas con censos de población y vivienda.

Para el Tratamiento de datos personales, **INFOTIC S.A.,** tendrá en cuenta las siguientes definiciones:

a) Autorización: consentimiento previo (o concurrente) expreso e informado del Titular para autorizar y permitir el Tratamiento de sus datos personales.

b) Base de datos: conjunto organizado de datos personales que sea objeto de Tratamiento.

c) Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[1]

d) Dato público: dato calificado como tal según los mandatos de la ley o la Constitución. Entre otros, son los datos relativos al estado civil de las personas, su oficio o profesión, su calidad de comerciante o servidor público. Por su naturaleza, los datos públicos son aquellos que están contenidos en registros públicos, gacetas, boletines y sentencias judiciales debidamente ejecutoriadas no sometidas a reserva.

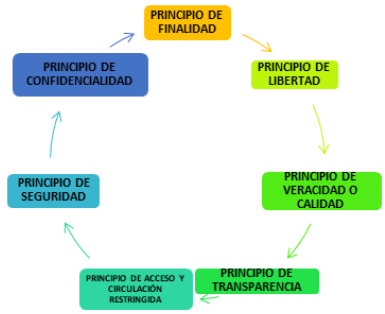
e) Encargado del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

f) Responsable del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre las bases de datos y/o el Tratamiento.

g) Titular: persona natural cuyos datos personales sean objeto de Tratamiento.

h) Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Para el desarrollo y aplicación del Tratamiento de datos personales, **INFOTIC S.A.**, seguirá los siguientes principios rectores:



a) Principio de finalidad: el Tratamiento debe obedecer a una finalidad legítima y ésta siempre debe ser informada al Titular.

b) Principio de libertad: el Tratamiento solo puede realizarse con el consentimiento previo (o concurrente) expreso e informado del Titular. Se debe precisar que los datos personales no pueden ser obtenidos o divulgados sin autorización, salvo que la Ley o las autoridades así lo permitan u ordenen.

c) Principio de veracidad o calidad: se debe procurar que la información objeto del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible. Los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.

d) Principio de transparencia: se debe garantizar que el Titular pueda obtener en cualquier momento y sin restricciones información acerca de la existencia de datos que le conciernan.

e) Principio de acceso y circulación restringida: el Tratamiento no puede ser irrestricto y seguirá estrictamente a los límites que se derivan de la naturaleza de los datos personales. Por tanto, salvo que se traten de datos públicos, los datos no podrán estar disponibles en Internet u otros medios de divulgación, salvo que el acceso sea controlable para que el mismo sea restringido solo a los Titulares y terceros autorizados.

f) Principio de seguridad: el Tratamiento se debe realizar con las medidas técnicas, humanas y administrativas que permitan otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

g) Principio de confidencialidad: las personas que realicen el Tratamiento deben garantizar la reserva de la información que no tenga la naturaleza de pública, incluso después de finalizada la labor del Tratamiento

II. TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES

De acuerdo con los términos de la Ley, existen diferentes categorías de datos personales. Por tanto, **INFOTIC S.A.** considera de gran importancia acoger, materializar y reconocer la existencia, alcance y contenido del concepto de dato sensible.

De conformidad con la Ley, los datos sensibles son aquellos cuyo uso indebido puede generar la discriminación o marginación de su Titular, tales como:

a. El origen racial o étnico del Titular.
b. La orientación política del Titular.
c. Las convicciones religiosas o filosóficas del Titular.
d. La pertenencia a sindicatos, ONG, organizaciones de derechos humanos, que promuevan intereses políticos o grupos de oposición.
e. Información relativa a la salud del Titular.
f. La inclinación sexual del Titular.
g. Datos biométricos del Titular.

INFOTIC S.A., se acoge a la regla general según la cual el Tratamiento de datos sensibles está prohibido por la Ley, salvo en los siguientes casos:

a. Cuando el Titular ha autorizado expresamente el Tratamiento.
b. Cuando el Tratamiento sea necesario para salvaguardar el interés vital del Titular.
c. Cuando el Tratamiento sea efectuado por una fundación, ONG, asociación o cualquier organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical.

d. El Tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e. El Tratamiento obedezca a una finalidad histórica, estadística o científica. En este caso, se deben suprimir las identidades de los Titulares.

El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, siempre que no se trate de datos de naturaleza pública. No obstante, **INFOTIC S.A.**, tiene en cuenta que la Ley no impone una prohibición absoluta del Tratamiento de datos personales de niños, niñas y adolescentes, pues ello daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, y lo que procurará **INFOTIC S.A.** en el Tratamiento de datos personales de menores, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el hábeas data.

En conclusión, los datos de los niños, las niñas y adolescentes pueden ser objeto de Tratamiento por parte de **INFOTIC S.A.**, siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente se responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular.

III. AUTORIZACIÓN – DEBER DE INFORMACIÓN – DERECHOS DE LOS TITULARES

Siempre que vaya a realizar Tratamiento de datos personales, **INFOTIC S.A.**, requerirá la autorización previa (o concurrente) e informada del Titular. La mencionada autorización debe ser obtenida por cualquier medio que pueda ser objeto de consulta posterior, ya sea un medio físico o electrónico.

No se necesita la autorización del Titular para el Tratamiento cuando se trate de:

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

b. Datos de naturaleza pública.

c. Casos de urgencia médica o sanitaria.

d. El Tratamiento de datos se realice para fines históricos, estadísticos o científicos.

a. Datos relacionados con el Registro Civil de las personas.

Al momento de solicitar la autorización del Titular, **INFOTIC S. A.**, le informará de manera clara y expresa:

a. El Tratamiento de los datos y su finalidad.

b. Si se trata de datos sensibles o de menores, el derecho a decidir si se suministra o no la información solicitada.

c. Los derechos que le asisten como Titular.

d. La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

INFOTIC S.A., conservará copia y prueba del cumplimiento del deber de información, así como del cumplimiento del deber de solicitar la autorización del Titular.

Al cumplir el deber de información, **INFOTIC S.A.**, informará de modo expreso a los Titulares que sus derechos son:

a. Derecho a conocer, actualizar y rectificar sus datos personales.

b. Derecho a solicitar prueba de la autorización otorgada para el Tratamiento.

c. Derecho a solicitar información respecto al uso que se le ha dado a sus datos personales.

d. Derecho a presentar quejas ante la Superintendencia de Industria y Comercio.

e. Derecho a revocar la autorización otorgada o la supresión de los datos.

f. Derecho a acceder de forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

I. **IV.PROCEDIMIENTOS PARA CONSULTAS Y RECLAMOS**

Para efectos de consultas y reclamos, **INFOTIC S.A.**, habilitará uno o varios medios para que los Titulares, sus herederos o representantes, verifiquen la existencia de información personal que se encuentre registrada las bases de datos de **INFOTIC S.A.**, consulten el Tratamiento que se le ha dado a dicha información, conozcan las finalidades que justifican este Tratamiento y soliciten la actualización, rectificación o supresión de estos datos personales.

La información se deberá proporcionar en su integridad y se debe conservar prueba de la atención efectiva a la consulta o reclamo.

Todas las consultas deben ser atendidas en un término que no sea superior a diez (10) días hábiles contados a partir del día en que se reciba la solicitud, siendo éste el primer día del término. Si no fuera posible atender la consulta en el término indicado, se deberá informar al interesado cuáles son los motivos de la demora y se debe señalar la fecha en que se dará respuesta a la consulta. De

cualquier manera, la nueva fecha no puede ser superior a cinco (5) días hábiles siguientes al vencimiento del término de diez (10) días.

Las personas a las que se les podrá suministrar la información son:

a. Los Titulares, sus causahabientes o sus representantes legales.

b. 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.

INFOTIC S.A., implementará las medidas necesarias para garantizar que el acceso a la información se permita después de verificar la identidad del interesado. El acceso se otorgará de manera gratuita, sencilla y ágil. Así mismo, se permitirá la posibilidad de rectificar y actualizar los datos en línea.

Por otra parte, todos los reclamos deberán ser atendidos en un término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Si no fuera posible atender el reclamo en el término indicado, se informarán los motivos al interesado y se indicará la fecha en que se dará respuesta. En todo caso, la nueva fecha no puede ser superior a ocho (8) días hábiles siguientes al vencimiento del término de quince (15) días.

Previo a dar trámite a cualquier reclamo, se debe verificar la identidad del reclamante, quien debe ser el Titular, su causahabiente o su representante. Si el reclamante no es ninguna de las personas indicadas anteriormente, no se tramitará el reclamo.

Un reclamo completo debe contener, por lo menos:

a. Identificación del Titular y del reclamante (en caso que no sea el mismo Titular).

b. Descripción de los hechos que dan lugar al reclamo.

c. Dirección física o electrónica de notificación.

d. Documentos y anexos que se pretendan hacer valer en el curso del reclamo.

e. Petición u objeto del reclamo.

Si se presenta una reclamación, pero la misma está incompleta, es decir, si le hacen falta elementos esenciales para darle el debido trámite, dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo se deberá solicitar al interesado para que subsane la reclamación. Si transcurren dos (2) meses sin que el reclamante subsane la reclamación, se entenderá que ha desistido de la misma.

Si se recibe un reclamo, pero no se tiene la competencia para resolverlo, se deberá enviar el mismo a quien corresponda en un término no mayor a dos (2) días hábiles y se informará al interesado de dicha situación.

Cuando se solicite la supresión de datos, la misma no podrá realizarse cuando:

a. Sea una obligación legal o contractual conservar dichos datos.

b. Conservar los datos sea imprescindible para salvaguardar los intereses del Titular o el interés público.

c. La supresión dificulte o entorpezca el ejercicio de las funciones de las autoridades administrativas o judiciales.

Cuando se solicite la revocatoria de la autorización, es preciso que el interesado informe con precisión si la revocatoria es total o parcial. La revocatoria de la autorización es parcial cuando el interesado manifiesta que desea revocar el Tratamiento de datos personales para ciertas finalidades específicas como aquellas publicitarias, de concursos, de estudios de consumo, etc. La revocatoria de la autorización es total cuando se solicita que se detenga el Tratamiento de datos personales para todas las finalidades autorizadas.

V.DEBERES DE LOS RESPONSABLES Y ENCARGADOS

INFOTIC S.A. cumplirá estrictamente los siguientes deberes de acuerdo a la calidad que ostente respecto al Tratamiento de los mismos en cada caso concreto:

5.1. CUANDO INFOTIC S.A. ACTUE COMO RESPONSABLE RESPECTO DEL TRATAMIENTO DE LOS DATOS TENDRÁ LOS SIGUIENTES DEBERES:

DEBERES DE INFOTIC S.A. COMO RESPONSABLE DE LOS DATOS	Garantizar al Titular el derecho al hábeas data.
	Solicitar y conservar copia de la autorización.
	Informar al Titular sobre la finalidad del Tratamiento y los derechos que le asisten.
	Conservar la información bajo condiciones de seguridad idóneas.
	Garantizar que la información que se suministre al Encargado sea veraz, completa, exacta, actualizada, comprobable y comprensible.
	Actualizar la información, comunicando oportunamente al Encargado todas las novedades respecto de los datos que previamente se le hayan suministrado y adoptar medidas para que la información se mantenga actualizada.
	Rectificar la información cuando sea incorrecta e informar al Encargado.
	Únicamente proporcionar al Encargado datos cuyo Tratamiento esté autorizado.
	Exigir al Encargado el respeto a las condiciones de seguridad y privacidad de la información del Titular.
	Tramitar las consultas y reclamos dentro de los términos de la Ley.
	Adoptar el presente Manual interno de políticas y procedimientos para garantizar el cumplimiento de la Ley.
	Una vez se haya presentado reclamación, informar al Encargado cuando determinada información se encuentre en reclamación por parte del Titular o interesado.
	Informar al Titular sobre el uso dado a sus datos personales.
	Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio) cuando se presenten violaciones a los códigos de seguridad y exista riesgo para la información de los Titulares.
	Cumplir con las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

5.2 CUANDO INFOTIC S.A. ACTUE COMO ENCARGADO RESPECTO DEL TRATAMIENTO DE LOS DATOS TENDRÁ LOS SIGUIENTES DEBERES

DEBERES DE INFOTIC S.A. COMO ENCARGADO DE LOS DATOS	Garantizar al Titular el derecho al hábeas data.
	Conservar la información bajo condiciones de seguridad idóneas.
	Realizar oportunamente la actualización, rectificación o supresión de los datos.
	Actualizar la información reportada por los responsables dentro de los cinco (5) días hábiles contados a partir de su recibo
	Tramitar las consultas y reclamos dentro de los términos de la Ley.
	Adoptar el presente Manual interno de políticas y procedimientos para garantizar el cumplimiento de la Ley.
	Registrar en la base de datos la leyenda “reclamo en trámite” en los términos de la Ley.
	Insertar en la base de datos la leyenda “información en discusión judicial” una vez se haya notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad
	Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo ha sido ordenado por la Superintendencia de Industria y Comercio.
	Permitir el acceso a la información únicamente a personas que pueden tener acceso a ella.
	Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio) cuando se presenten violaciones a los códigos de seguridad y exista riesgo para la información de los Titulares.
	Cumplir con las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

VI.SEGURIDAD DE LA INFORMACIÓN

INFOTIC S.A. adoptará todas las medidas técnicas, humanas y administrativas que sean indispensables para dotar de seguridad sus bases de datos, evitando su adulteración, pérdida, consulta, acceso no autorizado o fraudulento.

Entre otras, las medidas de seguridad adoptadas incluyen, pero no se limitan a:

a. Encriptar la prestación de nuestros servicios usando protocolos de seguridad.
b. Establecimiento de cláusulas de confidencialidad contractual con los empleados que van más allá de la duración misma del contrato.
c. Implementación de procesos de seguridad para verificar la identidad de las personas que acceden a la información ya sea de manera física o electrónica.
d. Actualización permanente de las medidas de seguridad para adaptarlas a la normatividad vigente.
e. Adopción de sistemas de seguridad de *firewalls* y detección de accesos no autorizados.
f. Monitoreo periódico de actividades sospechosas y mantenimiento físico y electrónico de las bases de datos.
g. Restricción interna de acceso a las bases de datos solo al personal autorizado.

POLÍTICAS DE SEGURIDAD INFORMÁTICA:

Objetivo

Constituir la base del entorno de seguridad de una empresa y definir las responsabilidades, los requisitos de seguridad, las funciones y las normas a seguir por los funcionarios de la entidad. De esta manera se protege la información de la empresa.

Es responsabilidad de los usuarios el aprovechamiento de los recursos informáticos ofrecidos para realizar las labores diarias dentro de la empresa.

El usuario es responsable de seguir las políticas de seguridad y procedimientos para el uso de los servicios, recursos informáticos, evitando cualquier práctica o uso inapropiado que pudiera poner en peligro la información de la empresa.

Alcance

- Esta política está dirigida a los funcionarios, consultores y demás miembros de INFOTIC S.A., incluyendo el personal vinculado con firmas que prestan servicios a la entidad que utilicen tecnología de información.
- Estas políticas aplican a equipos de cómputo propios de INFOTIC S.A. y de propiedad de personas que sean conectadas a la red de la entidad.
- La garantía del cumplimiento de esta política será responsabilidad de cada miembro de INFOTIC S.A. pues su desacato afecta a toda la entidad.
- No se permite el uso de los bienes y servicios informáticos para:
    - Llevar a cabo actividades fuera de la ley
    - Exportar software, información técnica en contra de leyes de control regional o internacional.
    - Hacer copia no autorizada de material protegido por derechos de autor.
    - Fines particulares en ningún momento.
    - Violar esta u otras políticas o reglamentos internos de la empresa.
    - Utilizar los recursos sin tener autorización o autoridad para hacerlo.
    - Permitir o facilitar que usuarios no autorizados hagan uso de los recursos de la empresa.
    - Utilizar los discos duros para almacenar archivos de música, fotos, videos, juegos o similares.
    - Utilizar memorias USB, DVD, CD, cámaras, celulares o cualquier otro dispositivo cuyo contenido sea desconocido en el equipo, sólo debe tener acceso a estas unidades externas el administrador del sistema, debido a que pueden contener virus, robar la base de datos, ingresar troyanos, realizar posibles fraudes, etc.
    - Utilizar dispositivos USB, disquetes o CD prestados por alguien para instalar programas o abrir archivos, ya que este proceso es inseguro e igualmente sólo lo debe hacer la persona encargada de sistemas.
    - Entregar, distribuir o divulgar a terceros información confidencial reservada o estratégica de la entidad, salvo autorización previa y expresa y que tenga que ver con el cumplimiento de las funciones de cada empleado.
    - Usar, alterar o acceder sin autorización a los datos de otros usuarios.
    - Suplantar a otras personas, haciendo uso de las claves de acceso ajenas a los servicios.
    - Interceptar o alterar la información que se transmite.
    - Sacar o tomar prestados los recursos informáticos sin la debida autorización.
    - Interferir deliberadamente el sistema o el trabajo de otros, por ejemplo, ejecutando códigos dañinos tales como virus.
    - Acceder remota o directamente a un equipo sin el debido permiso del usuario, cuando se requiera acceder remotamente a un equipo de la empresa, se deberá utilizar únicamente conexiones seguras creadas por el área de sistemas.
    - Realizar tareas no relacionadas con actividades propias de la empresa.
    - Utilizar la infraestructura de tecnología de información de INFOTIC
    - S.A. para conseguir o transmitir material con ánimo de lucro.
    - Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de INFOTIC S.A.
    - Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran, acceder a datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado.
    -
    - Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad informática pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.
    - Instalar software sin estar debidamente autorizado para ello, sea o no, propiedad de la empresa.
    - Dejar equipos que contengan información de la empresa en sitios diferentes a ella.
- Se debe tener en cuenta el manejo de un antivirus de la siguiente manera:
    - Todos los equipos pertenecientes a la empresa deben tener un antivirus efectivo y actualizado.
    - Los equipos con acceso a Internet deberán actualizar y ejecutar el antivirus de manera constante.
    - Todos los equipos de la empresa, deberán ser examinados en su totalidad, una vez a la semana, por el antivirus.
    - Revisar todo elemento que ingrese a la entidad.
    - Cualquier archivo de origen ajeno al equipo, debe ser revisado por el antivirus, sin importar el medio de almacenamiento de éste (CD, USB o compartido en red).
    - Revisar el contenido de archivos comprimidos y correos electrónicos.
    - Si durante el proceso de revisión de algún medio de almacenamiento se detecta algún virus, el archivo debe ser inmediatamente eliminado.
    - Los equipos que no son de propiedad de INFOTIC S.A. pero que de igual manera se conecten a la red deben ejecutar un software de antivirus actualizado.
- No compartir carpetas, solo cuando sea absolutamente necesario y con las personas que lo necesiten, dándole seguridad a los datos. Tarea que deberá realizar el administrador de la red.
- Realizar copias de seguridad:
    - Se deben realizar copias de seguridad de los sistemas de información en forma periódica (diaria, semanal, quincenal o mensual) dependiendo de la importancia de la información, estas a su vez deben tener otra copia que será almacenada en un lugar externo a la sede.
    - Se deben realizar copias de seguridad de las bases de datos del sistema de información de Cobro Coactivo en forma mensual.
    - Se deben realizar copias de seguridad de las bases de datos del sistema de información de Patios y Grúas en forma mensual.
    - Se debe realizar copias de seguridad de los servidores locales y carpetas de cada usuario en forma quincenal o mensual dependiendo de la importancia de la información.
    - Backup de la Página Web: Todo el directorio raíz que contiene la estructura, base de datos, contenido y multimedia. En forma mensual.
- Tener en cuenta el uso de contraseñas seguras:
    - Todas las contraseñas son de carácter confidencial, intransferibles y de uso individual.
    - No compartir las contraseñas de acceso con otros usuarios de los sistemas.
    - No revelar las contraseñas o código de su cuenta por ningún medio de comunicación o directamente a otros (por ejemplo, su cuenta de correo electrónico, su usuario de bases de datos o permitir su uso a terceros para actividades ajenas a la misión de INFOTIC S.A. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario cuando la actividad se realiza desde el hogar (por ejemplo, computadores portátiles, teléfonos celulares).
    - No utilizar las funciones "recordar contraseña" que poseen algunas aplicaciones.
    - No escribir las contraseñas en ningún documento que se encuentre en su lugar de trabajo.
    - Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios
    - Para la definición de contraseñas, tener en cuenta lo siguiente:
        - Usar caracteres en mayúsculas y minúsculas (por ejemplo: a-z, A-Z)
        - Contener caracteres especiales (por ejemplo: 0- 9,^&*()_+|~=\`{}[]:";'<>?,./).
        - El establecimiento de una contraseña debe ser al menos de 8 caracteres.
        - Las claves de los usuarios con privilegios (administradores de servidores) deben cambiarse mínimo cada mes y las claves de los usuarios sin privilegios deben cambiarse mínimo cada dos meses.
        - No debe estar basada en información personal, nombres de familia, número de cédula, fecha de nacimiento etc.
        - Las contraseñas no deben ser nunca almacenadas en un equipo de cómputo.
        - Se debe tratar de crear contraseñas que puedan ser recordadas fácilmente y que pueda escribirse rápidamente, pero que la contraseña no sea una palabra que pueda ser encontrada en un diccionario.
- No se debe dejar ningún tipo de archivo ni de menú abierto mientras se abandona el puesto de trabajo.
- No ingresar información al sistema en horarios no autorizados.
- Esta información no puede ser conocida por terceros sin autorización del responsable de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave

a terceros o a los sistemas y/o los procesos.

- Respecto del uso de Correo Electrónico de la Entidad:
  - Está prohibido enviar mensajes de correo no solicitados, incluyendo correos basura (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial desde el correo interno (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
  - Está prohibido generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
  - Está prohibido el envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.
  - No utilizar el Internet para descargas de programas o trabajos de dudosa procedencia.
  - No utilizar las cuentas de correo corporativas para recibir o enviar correo personal.
  - No se debe utilizar el correo personal para enviar o recibir información de la entidad.
- El uso de software deberá regirse por los siguientes términos:
  - El software que se debe usar en los equipos de cómputo debe ser completamente legalizado (compra de licencia para el uso del software).
  - El uso de Software libre está permitido donde el funcionario deberá solicitarlo a su encargado explicando el uso y la descripción del software a instalar.
  - El área de sistemas debe mantener bajo su resguardo el software que se utiliza en INFOTIC S.A., los medios de instalación CD originales, licencias, manuales y garantías de equipos.
  - Se deben establecer los controles necesarios para mantener la información protegida. (Firewall, antivirus, monitoreo de puertos, protocolos, copias de respaldo, mantenimiento de equipos, software, red. Se recomienda el uso de criptografía para la información que los usuarios consideren sensitiva o vulnerable.
- Respecto de la seguridad del software:
  - Está prohibido el uso de software malicioso (virus, troyanos, keyloggers, exploits, shell inversa o puerta trasera, escáner de puertos, sniffers), sólo excluye pruebas de seguridad interna.
  - Se deberá pedir autorización para la instalación de herramientas de Pentesting, las cuales deben ir de acuerdo con el plan de auditoría establecido por INFOTIC S.A.
  - Para bajar páginas de internet, archivos ejecutables, etc., definir siempre en el equipo de cómputo una carpeta o directorio para recibir el material. De ese modo aseguramos que todo lo que bajemos de internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.
  - Nunca abrir un adjunto de un email sin antes chequearlo con el antivirus. Si el adjunto es de un desconocido que no da avisó previamente del envío del material, directamente borrarlo sin abrir.
  - Se deben tener copias de seguridad en dos sitios diferentes a la entidad.
- Para la actualización de software, tener en cuenta lo siguiente:
  - El software instalado debe ser actualizado cada vez que haya una actualización disponible si se considera necesario.
  - Las Actualizaciones Automáticas de los sistemas operativos deberán estar elegidas con la opción de notificación previa para descarga, a partir de esto seleccionar los paquetes de actualización relacionados con parches de seguridad y otras necesarias.
- Protección de la Información:
  - Para prevenir la pérdida de datos por corte abrupto de la energía eléctrica, los usuarios deben grabar periódicamente sus archivos de datos cuando se encuentre trabajando en cualquier herramienta o software de propósito específico.
  - No se debe compartir las tomas de su equipo con otros aparatos de diferente especificación como celulares, lámparas, secadores de cabello, brilladoras, taladros, impresoras, sumadoras. Estos pueden provocar cambios transitorios bruscos de voltaje, que pueden llegar a dañar el equipo o producir pérdida de información.
  - El equipo se debe conectar únicamente a tomacorrientes que pertenezcan al circuito eléctrico exclusivo para ellos, con protección contra sobrevoltajes transitorios (cortapicos).
  -
  - Cuando se presenten tempestades, los equipos se deben desconectar, pues las descargas eléctricas pueden ocasionar daños, especialmente si están conectados a una línea telefónica a través de módem.
  - En caso de tener que mover los equipos por cualquier razón verificar que estén apagados, evitar movimientos bruscos o traslados frecuentes que puedan ocasionar problemas; en consecuencia, para evitar que se dañen.
  - Nunca conecten o desconecten periféricos o dispositivos como impresoras, monitores, teclados cuando el equipo está prendido, esto podría ocasionar que el puerto o tarjeta en donde se conectan dichos periféricos se dañen.
  - Almacenar, solo los archivos de datos que sean estrictamente necesarios y borrar o descargar aquellos que no se requieran de acuerdo con la necesidad y la importancia de cada uno de ellos.

RECOMENDACIONES

- Para dar de baja a un elemento informático debe solicitarse el concepto técnico del área de sistemas.
- Todo elemento informático que ingrese a la entidad debe ser entregado al área de sistemas para su debido chequeo, registro, resguardo o asignación de usuario o uso respectivo.
- Toda adición tanto de software como de hardware a los equipos de cómputo debe solicitarse a la división de sistemas.
- El uso de recursos o servicios informáticos de INFOTIC S.A. está sujeto a monitoreo por parte del área de sistemas.
- La creación de usuarios, el acceso y privilegios deben ser autorizados por el administrador del sistema.
- Por seguridad, se deben dar los mínimos permisos sobre cada recurso informático a los usuarios que permitan su normal operación.
- Cada usuario del equipo informático en forma compartida o individual son responsables de éste, de velar por su integridad, del uso que se le da a la cuenta de red, correo y acceso a Internet. Al igual que los datos son de su exclusiva responsabilidad.
- Los usuarios deben asignar a los directorios, subdirectorios y archivos, nombres que tengan relación clara y directa con el contenido de los mismos.
- No utilizar las unidades de red para manejo de información personal, fotos, música, videos.
- No comer cerca de teclados, tomar bebidas, colocar vasos sobre o cerca de los equipos ni fumar cerca de éstos, ya que se pueden ocasionar daños en los integrados
- Los dispositivos (token) utilizados para ingreso a páginas de bancos deben estar en sitios seguros.
- Las chequeras, CDT y sellos deben estar en sitios seguros fuera del alcance de personas no autorizadas.

VII.ÁREA ENCARGADA DE LA PROTECCIÓN DE DATOS PERSONALES

INFOTIC S.A. designa al área de Calidad o quien corresponda para que en adelante asuma, en adición a sus otras funciones, la de garantizar la protección de datos personales a los Titulares y darles trámite oportuno a sus solicitudes.

Estas funciones se desarrollarán con el apoyo del área jurídica. Por tanto, el área de Calidad o quien corresponda será la responsable al interior de **INFOTIC S.A.** de adoptar, implementar y cumplir las directrices de la Ley 1581 de 2012, el Decreto 1377 de 2013 y aquellas que los adicionen o modifiquen

VIII.LEGISLACIÓN APLICABLE Y VIGENCIA

Las políticas contenidas en el presente documento se elaboraron teniendo en cuenta el artículo 15 de la Constitución Política, las disposiciones contenidas en los artículos 15 y 20 de la Constitución Política, la Ley 1266 de 2008, la Ley 1581 de 2012, los Decretos Reglamentarios 1727 de 2009, 2952 de 2010 y el Decreto Reglamentario parcial No 1377 de 2013, y las Sentencias de la Corte Constitucional C – 1011 de 2008, y C - 748 del 2011.

[1]Esta definición, aunque es amplia, concuerda en términos generales con la línea jurisprudencial que la Corte ha desarrollado en la materia, así como con la definición adoptada en la Ley 1266 sobre el dato personal financiero. Se debe tener en cuenta que las características del dato personal son: i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Elaboró:	Revisó:	Aprobó:
Michael Avila Soporte Técnico	Maria Carolina Guerrero Secretaría General	Adolfo Tejada Presidencia