

1. OBJETIVO

Definir los lineamientos para garantizar la protección de los datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de ACT Telemática S.A., garantizando el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se hubiera recogido sobre ellas en bases de datos o archivos en concordancia con la normatividad vigente.

2. ALCANCE

Aplicará para todos aquellos datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de ACT Telemática S.A., respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las responsabilidades de la Compañía y de sus colaboradores en el manejo y tratamiento de los datos personales que reposen en sus bases de datos y archivos.

3. RESPONSABLES

- **ENCARGADO DEL TRATAMIENTO DE DATOS.**

El responsable del tratamiento de datos personales es **ACT TELEMÁTICA S.A.**, con domicilio en Bogotá, en la Carrera 47a N. 93 - 26 La Castellana. Oficina de Administración, Teléfono: 60+(1) 6210408.

- **RESPONSABLES INTERNOS**

Los líderes de Gestión Humana, Compras y Gerencia Comercial, para atender las peticiones, consultas y reclamos, donde el titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir los datos o revocar la autorización.

4. DEFINICIONES

Titular de la información:	Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos, sujeto del derecho de hábeas data y demás derechos y garantías.
Fuente de información:	Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación o de un servicio o de cualquier otra índole y que, debido a autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.
Titular:	Persona natural cuyos datos personales sean objeto de Tratamiento.
Entidad Titular:	Persona jurídica cuyos datos personales sean objeto de Tratamiento.
Dato personal:	Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente política. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Autorización:	Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de los datos personales.
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 datos.
Tratamiento:	Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión.
Autorización del titular:	El tratamiento requiere una autorización previa e informada del titular, 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.

Aviso de privacidad:	Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
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 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.
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 estos 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.

5. CONSIDERACIONES GENERALES

5.1 PRINCIPIOS

ACT Telemática S.A., aplicará dentro de su política de tratamiento de datos, para efectos de interpretación y aplicación, los principios constitucionales y legales en el tratamiento de la información como son:

- **Principio de legalidad en materia de Tratamiento de datos:** El tratamiento a que se refiere la ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
- **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- **Principio de libertad:** El Tratamiento sólo 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.
- **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de 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.
- **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 presente 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 presente 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 presente ley.

- **Principio de seguridad:** La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, 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.
- **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 esta.

5.2 DERECHOS DE LOS TITULARES

Según el artículo octavo de la Ley Estatutaria 1581 de 2012, los titulares de los datos tendrán derecho a:

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la ley;
- A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
- A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
- A las bases de datos y archivos de información periodística y otros contenidos editoriales;
- A las bases de datos y archivos regulados por la Ley 1266 de 2008;
- A las bases de datos y archivos regulados por la Ley 79 de 1993;
- Legitimación para el ejercicio del derecho del titular;
- Conocer, actualizar y rectificar sus datos personales;
- Solicitar prueba de la autorización otorgada;
- Ser informado, previa solicitud, respecto del uso que les ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley;
- Revocar la autorización y/o solicitar la supresión del dato;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, a través del correo electrónico protecciondatos@acttelematica.com.co encargado de peticiones, consultas y reclamos.

Los derechos de los titulares podrán ejercerse por las siguientes personas:

- Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición de la Compañía;
- Por los causahabientes del Titular (en los casos que éste falte por muerte o incapacidad), quienes deberán acreditar tal calidad;
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o poder correspondiente;
- Por estipulación a favor de otro o para otro.

5.3 DEBERES DE ACT TELEMÁTICA S.A.

Los responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, 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, pérdida, 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 de conformidad con lo previsto en la ley;
- i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- j) Informar al Encargado del Tratamiento 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 mediante los canales impuestos por la compañía (correo electrónico y documento físico). 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;
- l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

6. POLITICAS

POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

ACT TELEMATICA S.A., Organización de carácter privado, con personería jurídica reconocida con NIT N°. 830.023.404-2, domiciliada en la ciudad de Bogotá en la Carrera 47ª N°. 93-26 y con sucursales en el territorio Colombiano, ubicadas en Barranquilla, Cartagena, Cali, Ibagué, Medellín, Montería, Neiva, Ibagué, Pereira, Sincelejo, Tunja, Yopal y Villavicencio, en cumplimiento de la normatividad vigente adopta las siguientes políticas de tratamiento de datos personales, en los términos de la ley 1581 de 2012, decreto 1377 de 2013 y circular 003 del 1 de agosto del 2018.

La protección de datos personales según la Constitución Política de Colombia (1991) en el Artículo 15 (Modificado Acto Legislativo 2003):

“...En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables.

Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley...”

La compañía en labor por ejercer su actividad económica, mediante los procesos administrativos y/o comerciales, conoce, trata y almacena datos personales situación que genera una responsabilidad para el adecuado manejo de estos. Es así como, la compañía da cumplimiento al artículo 15 de la Constitución Política de Colombia (1991), Ley 1581 de 2012 y el Decreto 1377 de 2013.

Serán objeto de protección, los datos de aquellas personas y empresas que, en ejercicio de cualquier actividad, directa o indirecta, incluyendo las laborales y comerciales, sean estas permanentes u ocasionales, puedan suministrar cualquier tipo de información o dato personal a la compañía, quien actúa en calidad de responsable del tratamiento de datos personales, y quien permitirá al titular de la información, conocerla, actualizarla y rectificarla.

POLITICA DE DESTRUCCIÓN DE INFORMACIÓN

ACT Telemática S.A., es consciente de la prudencia y responsabilidad en el momento de deshacerse de los datos. Por lo tanto, para la data física se hace una destrucción manual y para la electrónica un borrado seguro electrónico utilizando un software de destrucción aconsejado y administrado por el Proceso de Servicios IT.

POLÍTICA DE USO DE CAMARAS DE SEGURIDAD Y VIGILANCIA

Como medida de seguridad para la protección de los colaboradores, contratistas, visitantes y de la propiedad pública de la empresa, existe un sistema de seguridad y vigilancia electrónica grabada mediante el uso de cámaras de video. Las grabaciones podrán ser utilizadas para identificar aquellas personas que puedan haber cometido actos delictivos o incurran en comportamiento o actividades dirigidas a la comisión de un delito, aunque éste no se configure, en contra de la propiedad o de sus colaboradores y/o visitantes.

Frecuencia de operación del sistema de seguridad y vigilancia

- a. El sistema de seguridad y vigilancia operará las veinticuatro (24) horas del día, todos los días del año, sujeto a cualquier desperfecto mecánico imprevisto.*
- b. Existe una notificación pública de la existencia de las cámaras de seguridad y las grabaciones.*
- c. En todo lugar en que operen las cámaras de video, dentro y en los alrededores de las instalaciones de la empresa, se despliegan avisos que indiquen que se opera un sistema de grabación las veinticuatro (24) horas del día, los siete (7) días de la semana.*
- d. Los avisos se ubicarán en el área de recepción de la empresa y en las áreas en que las cámaras de seguridad y vigilancia estén instaladas.*

Función y uso

- a. Las cámaras de seguridad estarán ubicadas en lugares visibles y deberán ser operadas éticamente; No deberán utilizarse para hacer acercamientos a persona alguna o dirigirse a actividades de estas personas, a menos que existan motivos fundados para creer que se está cometiendo un acto delictivo.*
- b. El sistema de vigilancia electrónica mediante el uso de cámaras de seguridad tendrá la capacidad para cubrir, vigilar, grabar y/o monitorear el exterior de las instalaciones, así como áreas comunes del interior*

de las oficinas administrativas propias, incluyendo áreas en donde se ubiquen los trabajadores y cualquier otro lugar que determine la administración por razones de seguridad.

- c. Las cámaras de seguridad no estarán ubicadas en las oficinas cerradas, los cubículos, los baños o cualquier otro lugar en donde exista una expectativa razonable de privacidad.
- d. Las imágenes se graban en formato digital.
- e. Cuando exista información de posibles actos ilegales o cuando la situación existente lo amerite, se programará el sistema de cámaras para grabar una o más escenas de forma continua.

Usos prohibidos

Quedan prohibidos los siguientes usos de vigilancia o instalaciones de cámaras de seguridad:

- a. Vigilancia mediante el uso de cámaras de seguridad ocultas.
- b. Vigilancia mediante el uso de cámaras de seguridad en oficinas, y salas de reuniones.
- c. Custodia, disposición, almacenamiento y conservación de las grabaciones
- d. La custodia y la disposición de las grabaciones digitales estarán a cargo del Proceso de Servicios IT, y de cualquier otra persona autorizada por dicha área con previa autorización de Gerencia quienes actuarán conforme a lo establecido en esta política.
- e. Las grabaciones que resulten del sistema de seguridad y vigilancia electrónica se archivarán y mantendrán en el servidor por un período máximo de 15 días, que es establecido por la compañía; Una vez transcurra el plazo establecido de grabación, el sistema automáticamente borrará para liberar memoria y continuar grabando.

Seguridad y acceso a sala de cómputo del sistema de seguridad y vigilancia

- a. El acceso a esta área estará restringido, sólo podrá acceder el personal autorizado por la Gerencia y Servicios IT.
- b. El encargado deberá mantener un registro de visitantes que tengan cualquier acceso y/o uso de las grabaciones de video.

Derecho de examinar las grabaciones

- a. La información recogida por medio del sistema de seguridad y vigilancia tendrá un uso restringido, su divulgación será controlada y conservación será limitada.
- b. Todo visitante, contratista o colaborador contra quien se lleve una acción criminal, civil o administrativa basada en una grabación, podrá solicitar examinar la misma, tramitando una solicitud de examen de la grabación ante el Gerente General.
- c. La solicitud deberá ser realizada por escrito, deberá expresar con detalle las razones que se tienen para examinar alguna grabación e indicar fecha y hora.
- d. Una vez se reciba una petición por escrito para examinar alguna grabación, el Gerente General con la recomendación del Proceso de Servicios IT, determinará si concede la misma, comunicando la determinación también por escrito.
- e. La entrega de duplicados de grabaciones a las autoridades investigativas o personas autorizadas debe constar en un recibo oficial firmado por el Gerente General y/o el personal designado por éste, así como por el receptor de la copia.

POLITICA DE USO DE EQUIPOS MULTIFUNCIONALES (IMPRESORA, FOTOCOPIADORA Y ESCÁNER).

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

- a. Se prohíbe el uso de documentos con información personal o datos confidenciales para fines de reciclaje.*
- b. Recoger inmediatamente todas las impresiones y/o fotocopias que contengan información confidencial para evitar su revelación.*
- c. Se debe imprimir solo lo que es estrictamente necesario.*
- d. Verificar el equipo multifuncional o impresora y las áreas adyacentes para asegurarse de que no queden copias adicionales. Si encuentra copias adicionales se deben destruir.*
- e. Los colaboradores deben asegurarse antes de retirarse del equipo multifuncional o de la impresora que tienen en su poder el documento original.*
- f. Si el equipo multifuncional o la impresora no está funcionando, borre el archivo de impresión.*
- g. Verificar el correo electrónico al que enviará la imagen digital (scanner) antes de hacerlo, para evitar el envío de documentos a destinatarios equivocados.*

7. DESCRIPCION DEL PROCESO

7.1 USO (FINALIDAD) DE LA INFORMACIÓN PERSONAL RECOPIADA EN LAS BASES DE DATOS:

La información personal que se ha recopilado. desde el inicio de sus operaciones y la que recopile en adelante, se usará para los siguientes fines:

- Envío de información y documentos relacionados con los servicios que debe prestar la administración.
- Remisión de información, requerimientos y notificaciones a todos los colaboradores, proveedores y contratistas, que se encuentran registrados en nuestras bases de datos.
- Respuesta a reclamaciones, requerimientos, peticiones y quejas de nuestros usuarios y visitantes.
- Envío de correo electrónico y demás mensajes de datos, informando sobre los eventos y actividades.
- Envío de felicitaciones y congratulaciones por fechas especiales.
- Comunicación sobre la existencia de sorteos, rifas, concursos, campañas publicitarias/comerciales y/o invitaciones a conciertos, actividades lúdicas o de entretenimiento que se realicen.
- Enviar encuestas de opinión sobre la satisfacción de clientes, usuarios y potenciales clientes.
- Análisis y segmentación de la información para elaborar estudios y estadísticas.
- Realizar encuestas y/o sondeos de opinión sobre productos y/o servicios.
- Dar cumplimiento a exigencias legales y requerimientos de autoridades judiciales.
- Monitoreo y control de seguridad de todas las personas que ingresan.
- Apoyo para la prestación de servicios de emergencia en caso de accidentes o contingencias.
- Soporte a labores de vigilancia.

ACT Telemática S.A., cuenta con cámaras de videovigilancia que recopilan información en formato de videos y fotografías y la almacenan, temporalmente, en dispositivos seguros de acceso restringido, cuyo manejo y tratamiento es responsabilidad se ajusta a los lineamientos de la presente política; estos videos se eliminarán automáticamente por el propio sistema, a medida que el espacio de almacenamiento lo exige. Cuando sea

requerido por autoridades competentes o se precise de la información para atender reclamaciones, quejas, sugerencias o para adelantar procesos administrativos internos. Así mismo ACT Telemática S.A., guardará los videos hasta el cumplimiento de su finalidad, luego de lo cual serán eliminados. Las personas que están facultadas para tener acceso al sistema de CCTV han suscrito con la empresa, documentos de confidencialidad y reserva de la información y se han comprometido al manejo apropiado y seguro de los datos. Se advierte a los visitantes que están siendo monitoreados y grabados por el circuito cerrado de televisión y se informa sobre sus derechos.

Garantizamos la recolección, almacenamiento, uso, transmisión y transferencia de sus datos personales a fin de cumplir y acreditar el cumplimiento de las obligaciones en materia de Seguridad y Salud en el Trabajo contempladas el Decreto 1072 de 2015 y Resolución 0312 de 2019 y cualquier otra norma asociada o que la modifique; ejecutando el control, seguimiento, monitoreo y vigilancia del cumplimiento de la vinculación del personal contratado así como realizar monitoreo preventivo de conocimiento de contrapartes, para mantener actualizada la información.

7.2 DATOS DE MENORES DE EDAD

ACT Telemática S.A, solo trata datos personales de menores de edad cuando sean necesarios y estos sean de naturaleza pública o provengan de la información suministrada por colaboradores o contratistas, al momento de su vinculación laboral o de prestación de servicios a la empresa; cualquier persona involucrada en el tratamiento de los datos personales de niños, niñas y adolescentes, velaran por el uso adecuado de los mismos.

En cumplimiento de lo anterior, se aplican y desarrollan los principios y obligaciones establecidos en el Decreto 1377 de 2013 y la Ley 1581 de 2012, conforme con lo establecido en el artículo 7 de la Ley 1581 de 2012 y, cuando el tratamiento cumpla con los siguientes parámetros y requisitos:

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

7.3 TRANSMISIÓN INTERNACIONAL DE DATOS.

Cuando aplique ACT Telemática S.A. realizara contratos de transmisión internacional de datos que contengan los siguientes parámetros:

- Los alcances del tratamiento a realizar por parte del Encargado.
- Las actividades que el Encargado realizará por cuenta del responsable para el tratamiento de los datos personales.
- El compromiso del Encargado a cumplir con la Política de Protección de Datos del responsable.

Dentro de las obligaciones del Encargado:

- a) Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
- b) Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- c) Guardar confidencialidad respecto del tratamiento de los datos personales.

En el contrato deberán indicarse otros aspectos de gran importancia como:

- a) Las medidas de seguridad tecnológicas o físicas que se implementaran sobre los canales a través de los cuales se realizará la transmisión de la información.

- b) Las finalidades autorizadas por el titular de los datos al responsable del Tratamiento, para que el Encargado solo ejerza tratamiento sobre los datos hasta donde dicha finalidad lo autorice.
- c) Las medidas de seguridad a tomar por el Encargado sobre la información, para evitar su acceso, adulteración, destrucción no autorizados o fraudulentos, como para evitar la fuga de información.
- d) Los canales para que los titulares ejerzan sus derechos frente al Encargado del Tratamiento.
- e) Las medidas a tomar sobre la información objeto de comunicación, una vez se termine la ejecución del contrato, bien sea su destrucción o devolución al responsable.
- f) La responsabilidad por el incumplimiento del contrato frente al manejo de la información personal, teniendo en cuenta que la materialización de cualquier riesgo sobre los datos personales como fuga, alteración o acceso no autorizado, entre otros, puede traer sanciones de carácter económico, a nivel administrativo e incluso penal

7.4 TERCERIZACIÓN DE SERVICIOS – CONTRATISTAS - INSPECCIÓN, VIGILANCIA Y CONTROL.

De acuerdo con las disposiciones legales en Colombia y en cumplimiento a las normas, la tercerización laboral o de servicios en ACT Telemática S.A. se ejecuta mediante contratos de prestación de servicios donde se estipulan las obligaciones del contratista y contratante, identificación de las partes, impuestos, cláusula de confidencialidad, tipo de contrato, seguridad social, dotación, garantías, descuentos, tiempo de ejecución y cláusulas compromisorias.

Inspecciones: De acuerdo con lo dispuesto en las normas colombianas, la empresa realizará auditorías internas para garantizar el funcionamiento y todo lo relacionado con la actividad que desempeñan los colaboradores, clientes y proveedores para garantizar el cumplimiento de protección de datos dentro de la empresa.

Casos en que no es necesaria la autorización: Información requerida por una autoridad o departamento administrativo en ejercicio de sus funciones legales o por orden judicial.

- a) Datos de naturaleza pública.
- b) Casos de urgencia médica o sanitaria.
- c) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- d) Datos relacionados con el registro civil de las personas.

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 Compañía. El reclamo lo podrá presentar el Titular, teniendo en cuenta la información señalada en el artículo 15 de la Ley 1581 de 2012, a través del correo electrónico protecciondatos@acttelematica.com.co

En cualquier caso, las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá la consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

8. ATENCIÓN DE CONSULTAS Y RECLAMOS

De acuerdo con las disposiciones de la compañía y normas establecidas en Colombia, a continuación, se enuncia el procedimiento que garantizara la especial atención a consultas y reclamos:

- a) Seguridad de la información: La compañía ha dispuesto un servidor dividido en las carpetas o archivos digitales que utiliza cada área. Para ello, únicamente tendrá acceso los colaboradores y líder de Proceso, de esta forma se garantiza el cuidado de los datos personales.
- b) Atención de consultas y reclamos: De acuerdo con lo dispuesto por ACT Telemática S.A. ha designado a los responsables de la protección de la información: Gerente Comercial y líderes de Gestión humana y Compras, donde los clientes, proveedores y colaboradores en casos de rectificación, actualización o supresión pueden dirigirse al correo electrónico protecciondatos@acttelematica.com.co
- c) El titular podrá actualizar, rectificar, corregir y suprimir y revocar su autorización de tratamiento de datos en cualquier momento, notificándose al correo electrónico protecciondatos@acttelematica.com.co ò dirigiendo un escrito a la oficina principal Carrera 47 a N.º 93-26, Bogotá D.C, Colombia

Si alguien requiere ejercer algún derecho es necesario detallar en el correo electrónico como mínimo la siguiente información:

- El nombre y domicilio del titular o cualquier otro medio para recibir la respuesta.
 - Los documentos que acrediten la identidad o la personalidad de su representante.
 - La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos
- d) Formatos y autorizaciones: La Compañía ha definido los formatos suficientes para cumplir las normas descritas en este documento entre ellos Gestión humana solicita la autorización de los colaboradores para tratar sus datos mediante un documento llamado Habeas Data, comercial y compras como protocolo hacen firmar de los terceros un formato de autorización de datos personales. Igualmente, al pie de las firmas de todos los colaboradores en correos electrónicos se encuentra una información de seguridad que respalda todo lo tratado bajo las cuentas en uso.
 - e) En cualquier momento y de manera gratuita el titular o su representante podrán solicitar a través de este correo electrónico la rectificación, actualización o supresión de sus datos personales, previa acreditación de su identidad. Los derechos de rectificación, actualización o supresión únicamente se podrán ejercer por:
 - El titular o sus causahabientes, previa acreditación de su identidad, confirmando cedula, y otros datos personales que ayuden a verificar su identificación.
 - Su representante, previa acreditación de la representación. Cuando la solicitud sea formulada por persona distinta del titular, deberá acreditarse en debida forma la personería o mandato para actuar; y en caso de no acreditar tal calidad, la solicitud se tendrá por no presentada.

9. ACTUALIZACIÓN DE BASES DE DATOS, REGISTROS, INFORMACIÓN, POLÍTICAS Y DEMÁS RELACIONADOS EN LA PLATAFORMA DE RNBD

ACT Telemática S.A. ingresara a la página Web de la Superintendencia de Industria y Comercio, (<https://www.sic.gov.co/registro-nacional-de-bases-de-datos>), Registro Nacional de Bases de Datos (RNBD), para actualización de bases de datos, registros, información, políticas y demás relacionados, por lo menos una vez al año, en cumplimiento de los requerimientos legales.

Antes de realizar el ingreso a la plataforma se deben tener en cuenta los siguientes componentes:

- Evaluar el tratamiento y condiciones de cada base de datos.
- Evaluar qué cambios se realizarán durante la actualización.
- Evaluar si es necesario actualizar la política y documentos relacionados.
- Contar con la aprobación del proceso a realizar por Gerencia

➤ **Disposiciones generales**

Copia de esta política deberá ser notificada al personal de la administración y se publicará un aviso de su existencia que indicará el procedimiento para obtener copia de esta, de manera que los visitantes y las personas que brindan servicios a establecimiento tengan conocimiento de éste.

➤ **Cláusula de salvedad**

Si cualquier disposición de esta política fuere declarada nula o inconstitucional por un tribunal con jurisdicción, dicha determinación o declaración no afectará, menoscabará o invalidará la validez de las restantes disposiciones y partes de este.

➤ **Aplicabilidad**

Las disposiciones de esta política se aplicarán a los colaboradores de la administración, los visitantes y los contratistas que visiten las instalaciones de la empresa, y a cualquier persona que acceda a las instalaciones y/o solicite acceso al sistema de vigilancia electrónica o a la información generada por el mismo.

10. CONTROL DE ACTUALIZACIONES DEL DOCUMENTO

Versión	Fecha Vigencia	Descripción General
0	15/12/2016	Creación del documento
1	29/06/2017	Revisión de criterios acorde a la normatividad vigente y las políticas a implementar por ACT Telemática.
2	26/09/2022	Se realiza el cambio de nombre POLITICA DE TRATAMIENTO DE LA INFORMACION, por POLITICAS CORPORATIVAS PARA EL TRATAMIENTO DE LA INFORMACION, dando cubrimiento a todas las políticas corporativas para el tratamiento de la información, se estructura documento acorde a HSEQ-PR-001, se incluye periodicidad de actualización de información, se elimina el equipo fax, puesto que no se cuenta con ese recurso para generar transmisión de datos; se coloca ampliación de las siguientes siglas ingresara a la página en internet de las Superintendencia de Industria y Comercio, (https://www.sic.gov.co/registro-nacional-de-bases-de-datos), al Registro Nacional de Bases de Datos (RNBD) Se incluye, el párrafo de Garantizamos la recolección, almacenamiento, uso, transmisión y transferencia de sus datos personales a fin de cumplir y acreditar el cumplimiento de las obligaciones en materia de Seguridad y Salud en el Trabajo contempladas el Decreto 1072 de 2015 y Resolución 0312 de 2019 y cualquier otra norma asociada o que la modifique; ejecutando el control, seguimiento, monitoreo y vigilancia del cumplimiento de la vinculación del personal contratado así como realizar monitoreo preventivo de conocimiento de contrapartes, para mantener actualizada la información.

ELABORO	REVISO	APROBO
Gerente Servicios IT	Gerente Administrativo y Financiero	Gerencia General