

Manual de Políticas y Procedimientos Habeas Data

ASOCIACIÓN COLOMBIANA DE TALENTO HUMANO Y ORGANIZACIONAL –
ACTHO

NIT 860.401.674-5 – (antes Asociación de Gestión Humana ACRIP Bogotá
y Cundinamarca)

Capítulo I

Políticas y Seguridad de Procedimientos

1. Base legal y ámbito de aplicación.

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD); **en el Decreto Único Reglamentario 1074 de 2015 (Libro 2, Parte 2, Título 2, Capítulos 25 y 26), que compiló los Decretos 1377 de 2013 y 886 de 2014 y reglamenta parcialmente la Ley 1581 de 2012; en el Título V de la Circular Única de la Superintendencia de Industria y Comercio (SIC), y en las demás normas que las modifiquen, adicionen o complementen.**

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 2
--	---	----------------------------------

de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la organización; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar por el cumplimiento de sus obligaciones, ACTHO designa al coordinador legal y de cumplimiento, como Oficial de Protección de Datos Personales y responsable de seguridad, encargado de atender las consultas y reclamos de los Titulares y de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en este manual.

En las ausencias temporales o definitivas del Oficial de Protección de Datos Personales, sus funciones serán asumidas por el Director administrativo de la Asociación o quien haga sus veces.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de ACTHO, así como a los encargados del tratamiento que traten datos personales por cuenta de ACTHO.

Todos los usuarios identificados en el presente documento de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Adicionalmente, hacen parte del marco normativo aplicable: la Ley 1266 de 2008, en lo pertinente; el Decreto 090 de 2018, sobre el Registro Nacional de Bases de Datos (RNBD); la Ley 2300 de 2023, sobre canales y horarios de contacto para gestiones de cobranza y envío de publicidad; la Circular Externa 002 de 2024 de la SIC, sobre tratamiento de datos personales en sistemas de inteligencia artificial; la Guía para la Implementación del Principio de Responsabilidad Demostrada y la Guía sobre Protección de Datos Personales en Sistemas de Videovigilancia expedidas por la SIC

Tipo de Norma	Número y fecha de expedición	Título	Expedida por	Aplicación específica
Ley Estatutaria	1581 de 2012	<i>"Por la cual se dictan disposiciones generales para la protección de datos personales".</i>	Congreso de la República.	Por medio de la cual 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 consagrada en el artículo 20 de la misma.
Ley	1273 de 2009	<i>Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"</i>	Congreso de la República.	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto	1377 de 2013	<i>'Por medio del cual se reglamenta parcialmente la ley 1581 de 2012'</i>	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	<i>'Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.'</i>	Presidente de la República de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria.

2. Definiciones establecidas en el artículo 3 de la LEPD y el capítulo 25 sección 1 artículo 2.2.2.25.1.3 del Decreto 1074 de 2015.

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autenticación correcta, generalmente mediante el ingreso de usuario y contraseña.

Autenticación: Procedimiento de verificación de la identidad de un usuario.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

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

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Contraseña: Señal secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autenticación de usuarios que permite el acceso autorizado.

Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autenticación.

Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato privado: Es el dato que por su naturaleza íntima o reservada solo es relevante para el Titular.

Dato semiprivado: Es el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio.

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 sensible aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

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

Identificación: Proceso de reconocimiento de la identidad de los usuarios.

Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

Incidente de seguridad: Violación de los códigos de seguridad o pérdida, robo y/o acceso no autorizado a información de una base de datos administrada por el Responsable o por su Encargado, que debe ser reportada a la SIC en los términos del numeral 12.1 del Capítulo II.

Perfil de usuario: Grupo de usuarios a los que se da acceso.

Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

Oficial de Protección de Datos Personales: Persona designada por ACTHO para atender las solicitudes de los Titulares y velar por la implementación efectiva de esta política y del principio de responsabilidad demostrada.

Responsable de seguridad: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad. • Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de 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 los datos.

Soporte: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

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 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.

3. Principios de la protección de datos.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1074 de 2015 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 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 revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD):

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 7
--	---	----------------------------------

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

- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.

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 conciernen. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

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 de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo 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 y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento 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. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga

acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el presente documento, de obligado cumplimiento para todo usuario y personal de ACTHO; Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

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 solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

Principio de responsabilidad demostrada: ACTHO adoptará medidas apropiadas, efectivas y verificables para cumplir las obligaciones de la LEPD y deberá estar en capacidad de demostrarlas ante la SIC cuando esta lo solicite, conforme a los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del Decreto 1074 de 2015. Para ello conservará evidencia de las autorizaciones, capacitaciones, auditorías, contratos de transmisión, registros de incidentes y de atención de consultas y reclamos.

4. Categorías especiales de datos.

4.1. Datos sensibles.

Los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Según el artículo 6 de la Ley Estatutaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

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.

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

El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, 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.

El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

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.

Aclaración: ACTHO no es una organización cuya finalidad sea política, filosófica, religiosa o sindical; en consecuencia, no se ampara en la excepción del literal c) anterior y solicitará siempre la autorización explícita del Titular para tratar datos sensibles, salvo los demás casos exceptuados por la ley. Al solicitarla, ACTHO: (i) informará al Titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento; (ii) le indicará de forma explícita y previa cuáles de los datos solicitados son sensibles y la finalidad específica de su tratamiento, y (iii) no condicionará ninguna actividad a que el Titular suministre datos sensibles (art. 2.2.2.25.2.3 del Decreto 1074 de 2015).

4.2. Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes solo procederá cuando dicho tratamiento cumpla con los siguientes requisitos (art. 7 de la LEPD, según la interpretación de la Corte Constitucional en la Sentencia C-748 de 2011, y art. 2.2.2.25.2.9 del Decreto 1074 de 2015):

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

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas

y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

4.3 Derechos de los Titulares.

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.
- Los derechos del Titular son los siguientes:

Derecho de acceso o consulta: Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

Derechos de quejas y reclamos: La Ley distingue cuatro tipos de reclamos:

Reclamo de corrección: El derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

Reclamo de supresión: El derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.

Reclamo de revocación: El derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

Reclamo de infracción: El derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento: salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones: El Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

Derecho a conocer, actualizar y rectificar: El Titular podrá conocer, actualizar y rectificar sus datos personales frente a ACTHO o sus encargados, en especial frente a datos parciales, inexactos, incompletos, fraccionados o que induzcan a error.

Derecho de revocatoria total o parcial: El Titular podrá revocar la autorización total o parcialmente, por ejemplo, solo respecto de las finalidades comerciales o de envío de publicidad, conservando las finalidades necesarias para su relación con ACTHO. La revocatoria y la supresión no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos (art. 2.2.2.25.2.6 del Decreto 1074 de 2015).

Derecho de acceso gratuito: El Titular podrá acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, en los términos del numeral 8.1.

5. Autorización de la política de tratamiento.

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular.

Modo de obtener la autorización. ACTHO solicitará la autorización a más tardar en el momento de la recolección de los datos, por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de manera razonable que la otorgó (art. 2.2.2.25.2.4 del Decreto 1074 de 2015). En ningún caso el silencio se asimilará a una conducta inequívoca.

Autorizaciones separadas por finalidad. ACTHO distinguirá entre: (i) las finalidades necesarias para la relación con el Titular (afiliación, inscripción, contratación o vínculo laboral) y para el cumplimiento de obligaciones legales, y (ii) las finalidades opcionales, que requerirán una autorización independiente, en casillas no marcadas previamente: envío de información comercial y publicitaria, transferencia de datos a patrocinadores y aliados, uso de imagen y voz con fines promocionales, segmentación o perfilamiento y tratamiento de datos sensibles. La negativa a autorizar finalidades opcionales no impedirá la afiliación, la inscripción o la vinculación.

Prueba de la autorización. ACTHO conservará prueba de cada autorización otorgada, que incluirá como mínimo: identificación del Titular, fecha y hora, canal utilizado, versión del texto aceptado y, cuando aplique, dirección IP o número telefónico, durante el tiempo que dure el tratamiento y el adicional necesario para atender reclamaciones (art. 2.2.2.25.2.5 del Decreto 1074 de 2015).

Aviso de privacidad y modelos de autorización. Cuando no sea posible poner a disposición del Titular la presente política, ACTHO le informará por medio del aviso de privacidad la existencia de la política y la forma de acceder a ella. Los modelos de aviso de privacidad y de autorización para formularios, correo electrónico y WhatsApp se incluyen en los Anexos 1 y 2.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

6. Responsable del tratamiento.

El responsable del tratamiento de las bases de datos objeto de esta política es la ASOCIACIÓN COLOMBIANA DE TALENTO HUMANO Y ORGANIZACIONAL – ACTHO (antes Asociación de Gestión Humana ACRIP Bogotá y Cundinamarca), entidad sin ánimo de lucro identificada con NIT 860.401.674-5, con domicilio en Bogotá D.C., cuyos datos de contacto son:

	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 13
--	---	----------------------------

Dirección: Carrera 7 # 73 – 55 Piso 2 Oficina 202, Bogotá D.C.

Correo electrónico: transparenciaydatos@actho.org

Teléfono: 6015188734 – 6015402020 – Celular: (+57) 318 280 0562

Página web: www.actho.org

6.1. las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de ACTHO son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el presente documento.
- Difundir el referido documento entre el personal afectado.
- Mantener este Manual actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la institución, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en este Manual, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada dos meses.

- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.
- Inscribir las bases de datos en el Registro Nacional de Bases de Datos (RNBD) y mantener su información actualizada en los plazos que fije la SIC, cuando ACTHO se encuentre obligada a ello (Decreto 1074 de 2015, Capítulo 26, y Decreto 090 de 2018).
- Reportar a la SIC, a través del RNBD, los incidentes de seguridad que afecten las bases de datos, dentro de los quince (15) días hábiles siguientes a su detección (arts. 17 lit. n y 18 lit. k de la LEPD), conforme al numeral 12.1 del Capítulo II.
- Suscribir contratos de transmisión con los encargados del tratamiento y mantener actualizado el inventario de encargados.
- Capacitar al personal en protección de datos personales al menos una vez al año y conservar evidencia de la capacitación.

7. Tratamiento y finalidades de las bases de datos

ACTHO, en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, ACTHO realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, transmisión de los datos a encargados del tratamiento, mediante el respectivo contrato de transmisión, y transferencia a otros responsables únicamente cuando el Titular lo haya autorizado de manera expresa o la ley lo permita. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información de ACTHO, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de ACTHO, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

La siguiente tabla presenta las distintas bases de datos y las finalidades asignadas a cada una de ellas.

BASES DE DATOS Y FINALIDADES

PROVEEDORES

Los datos serán utilizados con las siguientes finalidades: Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio; envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la Asociación; actuaciones administrativas, judiciales o extrajudiciales con naturales al vínculo obligacional suscrito, rastreo en bases de datos restrictivas tales como (policía, procuraduría, contraloría, SARLAFT – Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo, Programa de Transparencia y Ética Empresarial Integral y las demás que la normatividad colombiana disponga). ACTHO no tratará los datos para finalidades distintas de las aquí descritas sin informar previamente al Titular y, cuando se requiera, obtener una nueva autorización.

CLIENTES O ASOCIADOS

Esta base comprende: (i) afiliados personas naturales; (ii) personas de contacto de las empresas afiliadas (representantes legales, directivos y colaboradores de las áreas de gestión humana); (iii) participantes, asistentes, conferencistas y docentes de eventos, programas y actividades, y (iv) suscriptores de comunicaciones. Los datos de las personas de contacto de las empresas afiliadas son datos personales de dichas personas: la empresa afiliada declarará haberles informado esta política, y ACTHO les solicitará directamente la autorización cuando se requiera.

a) Finalidades necesarias para la relación y de cumplimiento legal: la gestión integral de la relación con los titulares, que abarca procesos de afiliación, registro, actualización, facturación, recaudo de cuotas, control de cartera y administración de bases de datos; la planeación, ejecución y memoria de eventos institucionales o realizados con terceros, incluyendo el registro de asistentes, control de acceso y la captación de imágenes, audios y videos para la memoria y el registro institucional de los eventos, previo aviso visible a los asistentes; la transmisión de datos a coorganizadores y proveedores logísticos que actúen como encargados, en la medida necesaria para el desarrollo de los eventos; el envío de comunicaciones relacionadas con la afiliación, la inscripción o el servicio solicitado; la realización de análisis estadísticos con datos agregados o anonimizado que contribuyan al cumplimiento del objeto social de la Asociación; el cumplimiento de obligaciones legales y regulatorias, en particular la prevención del lavado de activos, la financiación del terrorismo, la corrupción y el soborno transnacional, mediante la implementación articulada de sistemas de gestión del riesgo y programas de transparencia y ética

empresarial; la verificación y actualización de la información mediante consultas en bases de datos públicas y privadas, incluyendo antecedentes judiciales, disciplinarios, fiscales y reputacionales, en la medida en que sea necesario y proporcional para la gestión de los riesgos de LA/FT/FPADM y del Programa de Transparencia y Ética Empresarial. Asimismo, envío de información comercial, publicitaria, boletines e invitaciones de ACTHO por correo electrónico, SMS, WhatsApp u otros canales elegidos por el Titular, para llamadas y mensajes de texto publicitarios, el Registro de Números Excluidos de la CRC, Adicionalmente, para la segmentación, perfilamiento y estudios de comportamiento para personalizar la oferta de servicios

b) Finalidades opcionales, sujetas a autorización previa, expresa e independiente del Titular, que podrá revocar en cualquier momento sin afectar su afiliación o inscripción: transferencia de datos de contacto (nombre, cargo, empresa, correo electrónico y teléfono) a patrocinadores, aliados y coorganizadores, nacionales o internacionales, para que envíen información comercial de sus productos y servicios bajo sus propias políticas de tratamiento; cuando el receptor se encuentre en un país que no ofrezca un nivel adecuado de protección, la autorización deberá ser expresa e inequívoca (art. 26 de la LEPD), y (iv) uso de imagen, voz y testimonio en piezas promocionales y publicitarias.

c) Datos sensibles: ACTHO solo tratará datos sensibles de esta base cuando sean estrictamente necesarios (por ejemplo, necesidades de accesibilidad o requerimientos alimentarios por motivos de salud para la logística de un evento), con autorización explícita e informando al Titular el carácter facultativo de su respuesta.

TRABAJADORES

Esta base comprende trabajadores, aspirantes en procesos de selección, aprendices, practicantes, extrabajadores y, cuando aplique, sus beneficiarios y familiares.

Los datos serán utilizados con las siguientes finalidades: Solicitud de datos concernientes a identificación personal, información de contacto, datos de carácter académico, datos del historial laboral, profesional y financiero; desarrollar adecuadamente el proceso de registro y vinculación laboral; implementar acciones de bienestar laboral; difundir ofertas laborales para participar en procesos internos de selección de personal en la Institución; comunicar información institucional; ejecutar actividades con fines estadísticos; desarrollar adecuadamente el proceso de actualización de los datos; desarrollar los procesos de inscripción en congresos; eventos o seminarios organizados por la Institución; adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres hijos); citar a los aspirantes en proceso de selección a las entrevistas programadas, realización de visitas domiciliarias únicamente para los cargos críticos definidos por ACTHO y con autorización del aspirante, verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional; Suministro de

información a las empresas con la cuales se tiene convenio, al fondo de empleados, confección de artículos de dotación, envío de información a través de mensajes de texto y correos electrónicos, entrega y asignación de equipos a los colaboradores; redacción de informes de gestión humana; proceso de afiliación al sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios; entrega de referencias laborales, uso de imágenes fotográficas y videos con fines corporativos; obtención y suministro de datos de los hijos de los colaboradores en el desarrollo de actividades recreativas y de bienestar a través de la Instituciones o entidades aliadas, previa autorización de su representante legal y con respeto de su interés superior, evaluaciones de desempeño; generación de certificaciones laborales, de ascenso, traslado, entrevista de retiro, en procesos de auditoría y control interno y externo, en la entrega de reportes obligatorios institucionales en entrevistas de retiro, desactivación de sistemas de información, gestión de afiliación y retiro de fondos de empleados y cooperativas, informes de terminación de contrato laboral y reporte del mismo ante el sistema de seguridad social; tratamiento de datos sensibles únicamente para las siguientes finalidades específicas, con autorización explícita salvo cuando la ley la exceptúe: (i) datos biométricos (huella o reconocimiento facial) para el control de acceso y el registro de jornada, ofreciendo un mecanismo alternativo a quien no lo autorice; (ii) datos de salud para el Sistema de Gestión de Seguridad y Salud en el Trabajo, la gestión de incapacidades, restricciones y recomendaciones médicas y las afiliaciones al Sistema de Seguridad Social, y (iii) datos sobre discapacidad para la realización de ajustes razonables. Realizar la consulta de antecedentes, en forma proporcional al cargo y al nivel de riesgo, disciplinarios, policiales, penitenciarios, penales, reputacionales y mitigación del riesgo de la proliferación de armas de destrucción masiva, lo anterior, con la finalidad de implementar el Programa de Transparencia y Ética Empresarial, así las cosas, tomar las medidas pertinentes que emanen del Programa. Conservar registros históricos durante los plazos legales aplicables. Gestionar trámites como solicitudes, quejas y/o reclamos a través de los canales corporativos puestos a disposición. La toma de fotografías y videos para publicaciones en los canales web oficiales de la asociación, se deja constancia que estos son con fines netamente corporativos y están sujetos a supresión o modificación por parte de los titulares de la información.

7.1 Atención a los Titulares de datos

Hernán Darío Rincón Uribe, en su calidad de Oficial de Protección de Datos Personales, será el encargado de la atención de peticiones, consultas y reclamos. Los Titulares podrán ejercer sus derechos a través de los siguientes canales habilitados:

- **Correo electrónico:** transparenciaydatos@actho.org
- **Teléfono celular:** (+57) 318 280 0562. Teléfonos fijos: (601) 518 8734.

 Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 18
--	--	-----------------------------------

- **Radicación física:** Carrera 7 # 73-55, piso 2, oficina 202, Bogotá D.C., en horario de lunes a jueves entre las 8:00 de la mañana a 4:00 de la tarde y el día viernes entre las 8:00 de la mañana hasta la 2:00 de la tarde.
- **Formulario web** en www.actho.org

Las solicitudes recibidas por un canal o área distinta serán remitidas al Oficial de Protección de Datos Personales dentro de los dos (2) días hábiles siguientes. ACTHO llevará un registro de las consultas y reclamos recibidos, con su fecha de recibo, respuesta y término de atención.

8. Procedimientos para ejercer los derechos del Titular.

8.1. Derecho de acceso o consulta.

Según el capítulo 25 sección 4 del decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.
- Para consultas cuya periodicidad sea mayor a una por cada mes calendario, ACTHO solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.
- El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante solicitud dirigida a ACTHO por cualquiera de los canales señalados en el numeral 7.1, preferiblemente indicando en el asunto “ejercicio del derecho de acceso o consulta”. Para facilitar su trámite, la solicitud deberá contener los siguientes datos:
 - Nombre y apellidos del Titular.
 - Información que permita verificar la identidad del Titular (por ejemplo, que la solicitud provenga del correo electrónico o del teléfono registrado). Solo cuando existan dudas razonables sobre la identidad, o cuando actúe un representante, causahabiente o apoderado, se solicitará copia del documento de identidad y del documento que acredite dicha calidad.
 - Petición en que se concreta la solicitud de acceso o consulta.

 Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 19
--	---	-----------------------------------

- Dirección física o electrónica para recibir la respuesta.
- Documentos acreditativos de la petición formulada, cuando corresponda.
- El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:
 - Visualización en pantalla.
 - Por escrito, con copia o fotocopia remitida por correo certificado o no.
 - Correo u otros medios electrónicos.
 - Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por ACTHO.

Una vez recibida la solicitud, ACTHO resolverá la consulta en un plazo máximo de diez (10) días hábiles contados a partir del día siguiente a la fecha de su recibo. 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. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

8.2. Derechos de quejas y reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante escrito dirigido a ACTHO por cualquiera de los canales señalados en el numeral 7.1, indicando en el asunto “ejercicio del derecho queja o reclamo”, la solicitud deberá contener los siguientes datos:

Nombre y apellidos del Titular.

- Identificación del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
- Dirección para notificaciones, fecha y firma del solicitante.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 20
--	---	-----------------------------------

- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

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.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. ACTHO resolverá el reclamo en un plazo máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

8.3. Revocatoria de la autorización y supresión de datos.

El Titular podrá solicitar en cualquier momento, por los canales del numeral 7.1, la revocatoria total o parcial de su autorización o la supresión de sus datos, siguiendo el procedimiento de reclamos del numeral 8.2. La revocatoria parcial podrá referirse a una o varias finalidades específicas (por ejemplo, el envío de publicidad), caso en el cual ACTHO podrá continuar el tratamiento para las demás finalidades autorizadas. La solicitud no procederá cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos. Las solicitudes de retiro de listas de envío de publicidad se atenderán sin necesidad de más trámite a través del enlace o la palabra clave de baja incluidos en cada comunicación.

9. Medidas de seguridad

ACTHO, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

 Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 21
--	---	-----------------------------------

Por otra parte, ACTHO, mediante la suscripción de contratos de transmisión de datos personales (art. 2.2.2.25.5.2 del Decreto 1074 de 2015), exige a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

ACTHO mantendrá un inventario de encargados del tratamiento (Anexo 4), que incluirá a los proveedores de servicios tecnológicos y en la nube (correo electrónico, almacenamiento, CRM, plataformas de eventos, pagos, formularios y mensajería), el país donde se almacenan los datos y el contrato o las cláusulas que amparan la transmisión.

A continuación, se exponen las medidas de seguridad implantadas por ACTHO, que están recogidas y desarrolladas en este documento (Tablas II, III, IV y V).

TABLA II. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) Y BASES DE DATOS (AUTOMATIZADAS, NO AUTOMATIZADAS)

Auditoria

- Auditoría ordinaria (interna o externa) cada año.
- Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.
- Informe de detección de deficiencias y propuesta de correcciones.
- Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
- Conservación del Informe a disposición de la autoridad.

Gestión de documentos y soportes.

- Medidas tales como, destructora de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.
- Acceso restringido al lugar donde se almacenan los datos.
- Sistema de etiquetado o identificación del tipo de información.
- Inventario de los soportes en los que se almacenan bases de datos.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 22
--	---	-----------------------------------

- Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.

Control de acceso

- Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña.
- Lista actualizada de usuarios y accesos autorizados.
- Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados.
- Concesión, alteración o anulación de permisos por el personal autorizado.

Incidencias

- Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
- Procedimiento de notificación y gestión de incidencias.

Personal

- Definición de las funciones y obligaciones de los usuarios con acceso a los datos.
- Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.
- Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas.

Políticas y Procedimientos

- Elaboración e implementación del Manual de obligatorio cumplimiento para el personal.
- Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

 Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 23
--	---	-----------------------------------

TABLA III. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

Archivo

Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.

Almacenamiento de documentos.

Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Custodia de documentos

Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.

BASES DE DATOS AUTOMATIZADAS

Identificación y autenticación

1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.
2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.

Telecomunicaciones

Acceso a datos mediante redes seguras.

TABLA IV. MEDIDAS DE SEGURIDAD PARA DATOS PRIVADOS SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS AUTOMATIZADAS Y NO AUTOMATIZADAS

Auditoría

- Auditoría ordinaria (interna o externa) cada año.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 24
--	---	-----------------------------------

- Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.
- Informe de detección de deficiencias y propuesta de correcciones.
- Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
- Conservación del Informe a disposición de la autoridad.

Responsable de seguridad

- Designación de uno o varios responsables de seguridad.
- Designación de uno o varios encargados del control y la coordinación de las medidas del Manual políticas y procedimientos.
- Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.

Políticas y Procedimientos Habeas Data

- Controles al menos una vez al año de cumplimiento, consistente en la auditoria anual, así como la capacitación al personal mínimo una vez al año.

BASES DE DATOS AUTOMATIZADAS

Gestión de documentos y soportes

Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Control de acceso

Control de acceso al lugar o lugares donde se ubican los sistemas de información.

Identificación y autenticación

Mecanismo que limite el número de intentos reiterados de acceso no autorizados.

Incidencias

Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.

Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 25
--	---	-----------------------------------

TABLA V. MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

Control de acceso

- Acceso solo para personal autorizado.
- Mecanismo de identificación de acceso.
- Registro de accesos de usuarios no autorizados.

Almacenamiento de documentos

- Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.

Copia o reproducción

- Solo por usuarios autorizados.
- Destrucción que impida el acceso o recuperación de los datos.

Traslado de documentación

- Medidas que impidan el acceso o manipulación de documentos

BASES DE DATOS AUTOMATIZADAS

Gestión de documentos y soportes

- Sistema de etiquetado confidencial.
- Cifrado de datos.
- Cifrado de dispositivos portátiles cuando sean retirados.

Control de acceso

- Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
- Control del registro de accesos por el responsable de seguridad. Informe mensual.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 26
--	---	-----------------------------------

- Conservación de los datos: por el periodo que las leyes impongan.

Telecomunicaciones

- Transmisión de datos mediante redes electrónicas cifradas.

9.1. Encargados de seguridad

Los encargados de seguridad tienen las siguientes funciones:

Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del manual de Políticas y Procedimientos Habeas Data.

Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.

Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en este manual.

Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.

Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

Definir los tiempos dentro de los cuales se realizarán las auditorías, los cuales NO podrán ser superiores a un año.

Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.

Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

9.2. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de ACTHO, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

ACTHO, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de ACTHO se definen, con carácter general, según el tipo de actividad que desarrollan de acuerdo con sus funciones dentro de la institución y, específicamente, por el contenido de este Manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en este documento.

Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual de Políticas y Procedimientos Habeas Data. por parte del personal al servicio de ACTHO, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y la organización.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de ACTHO son las siguientes:

Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de ACTHO no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

Obligaciones relacionadas con las medidas de seguridad implantadas: Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.

- No revelar información a terceras personas ni a usuarios no autorizados.
- Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.

- No sacar información de las instalaciones de la organización sin la debida autorización.

Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.

Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los computadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades

Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o

comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la institución.

Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en este manual.

10. Transferencia de datos a terceros países.

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia en la de acuerdo con la circular 005 de 10 de agosto de 2017, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

Capítulo II

De Las Medidas de Seguridad

1. Cumplimiento y actualización.

Este es un documento interno de obligatorio cumplimiento para todo el personal ACTHO, con acceso a los sistemas de información que contengan datos personales.

Este manual de Políticas y Procedimientos Habeas Data, debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

2. Medidas de seguridad.

Las bases de datos son accesibles únicamente por las personas designadas por ACTHO, y referidas en el numeral 12 de este documento.

Los responsables de seguridad ACTHO, señalados en el numeral 12 del presente manual, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan las medidas de seguridad implementadas por ACTHO.

2.1 Medidas de seguridad comunes.

2.1.1 Gestión de documentos y soportes.

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 31
--	---	-----------------------------------

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el numeral 12 sobre bases de datos y sistemas de información del presente manual.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de estos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos.

La identificación de los documentos y soportes de contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de las personas.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El inventario de documentos y soportes de ACTHO debe incluirse como anexo del presente manual.

3. Control de acceso.

El personal de ACTHO solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en este manual.

ACTHO se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a ACTHO, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en el numeral 12 de este capítulo.

3.1 Ejecución del tratamiento fuera de la institución.

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera del lugar natural de trabajo, requiere una autorización previa por parte de ACTHO, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

3.2 Bases de datos temporales, copias y reproducciones.

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado en el numeral 12 puede realizar copias o reproducir los documentos.

3.3 responsable de seguridad.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

4. Auditoría.

Las bases de datos que contengan datos personales, objeto de tratamiento por ACTHO, clasificadas con nivel de seguridad sensible o privado, se han de someter, a una auditoría cada año, esta puede ser una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

ACTHO, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de estas.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 33
--	---	-----------------------------------

Las auditorías concluirán con un informe de auditoría que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias encontradas y la sugerencia de medidas correctoras o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El responsable de seguridad que corresponda estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctoras. Los informes de auditoría serán adjuntados a este manual y quedarán a disposición de la Superintendencia de Industria y Comercio.

5. Medidas de seguridad para bases de datos no automatizadas.

5.1 Archivo de documentos.

ACTHO, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el numeral 12 de este manual.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la institución.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso ACTHO, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el numeral 12 del presente manual.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, ACTHO, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente documento.

La descripción de las medidas de seguridad de almacenamiento se encuentra recogidas en el numeral 12 de este capítulo.

6. Acceso a los documentos.

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el numeral 12 del manual, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad en cuestión de ACTHO.

7. Medidas de seguridad para bases de datos automatizadas.

7.1 Identificación y autenticación.

ACTHO, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios se recogen en el numeral 12 de este documento.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y caracteres especiales. Siempre que la plataforma lo permita, se habilitará la autenticación de dos factores (2FA), en especial para el correo electrónico institucional y los sistemas que contengan datos sensibles. La política de contraseñas de ACTHO se encuentra en el numeral 12 del presente manual.

Por otra parte, ACTHO debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días. El periodo de vigencia de las contraseñas se recoge en el ya referido numeral 12.

ACTHO, también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el numeral 12 del manual.

8. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

El sistema de registro de entrada y salida debe ser anexado en el presente documento.

Las instalaciones de ACTHO son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; así mismo, han de cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde incluyen los datos.

ACTHO, tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual. Los locales e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el numeral 12 del presente documento.

Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

9. Copias de respaldo y recuperación de datos.

ACTHO, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez al bimestre, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este manual.

ACTHO, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses.

Los procedimientos de copia y respaldo se recogen en numeral 12 de este manual.

ACTHO, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de estos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento.

Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

10. Registro de acceso.

De los intentos de acceso a los sistemas de información de ACTHO, deberá guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter bimensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 37
--	---	-----------------------------------

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente en el presente documento.

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

11. Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

ACTHO, debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente manual de Políticas y Procedimientos Habeas Data para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

ACTHO, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el numeral 12 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de ACTHO se definen, con carácter general, según el tipo de actividad que desarrollan al interior de la institución, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el numeral 12 sobre bases de datos y sistemas de información. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente manual por parte del personal al servicio de ACTHO es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre las partes.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de ACTHO son las siguientes:

Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de estos.

Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos se anexarán en el presente manual.

- Las obligaciones relacionadas con las medidas de seguridad implantadas
- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados.
- Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.
- Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.
- Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de estos.

- Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
- Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los computadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades al interior de ACTHO.

Uso de herramientas de inteligencia artificial: Está prohibido ingresar datos personales de afiliados, participantes, proveedores o colaboradores en herramientas de inteligencia artificial que no hayan sido autorizadas por ACTHO o de uso institucional. El uso de herramientas autorizadas con datos personales requerirá que se realice en los aplicativos adquiridos por licencia por ACTHO o sean autorizados expresamente y requerirá una evaluación previa de riesgos y seguirá los lineamientos de la Circular Externa 002 de 2024 de la SIC.

Uso de mensajería instantánea: Las comunicaciones masivas por WhatsApp u otras aplicaciones se harán mediante listas de difusión, canales o herramientas empresariales que no expongan los números de los destinatarios a terceros. No se crearán grupos con Titulares sin su autorización.

- Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales propiedad de ACTHO
- Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el presente capítulo.

12. bases de datos y sistemas de información.

Las bases de datos almacenadas y tratadas por ACTHO se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

Base de datos	Nivel de seguridad
PROVEEDORES	Alto
CLIENTES O ASOCIADOS	Alto
TRABAJADORES	Alto

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de ACTHO.

Tabla II. Estructura de las Bases de datos

Nombre de la base de datos	PROVEEDORES
Responsable del tratamiento	ACTHO NIT: 860.401.674-5 Dirección: Carrera 7 # 73 - 55 Piso 2 Ofc 202, Bogotá D.C. Teléfono: (+57) 318 280 0562 Correo electrónico: transparenciaydatos@actho.org
Encargado de consultas y reclamos	Hernán Darío Rincón Uribe
Tipo de datos	Privada
Control de acceso físico	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	Bimensual

Nombre de la base de datos	CLIENTES O ASOCIADOS
Responsable del tratamiento	ACTHO NIT: 860.401.674-5 Dirección: Carrera 7 # 73 - 55 Piso 2 Ofc 202, Bogotá D.C. Teléfono: (+57) 318 280 0562 Correo electrónico: transparenciaydatos@actho.org
Encargado de consultas y reclamos	Hernán Darío Rincón Uribe
Tipo de datos	Sensible
Control de acceso físico:	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	Bimensual

Nombre de la base de datos	TRABAJADORES
Responsable del tratamiento	ACTHO NIT: 860.401.674-5 Dirección: Carrera 7 # 73 - 55 Piso 2 Ofc 202, Bogotá D.C. Teléfono: (+57) 318 280 0562 Correo electrónico: transparenciaydatos@actho.org
Encargado de consultas y reclamos	Hernán Darío Rincón Uribe
Tipo de datos	Sensible
Control de acceso físico:	Usuarios Autorizados
Control de acceso lógico	Usuarios y Contraseñas
Copias de respaldo	Bimensual

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

ACTHO, identifica en este manual, a los encargados del tratamiento, así como las condiciones del encargo. Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

12.1 Procedimiento de notificación, gestión y respuesta ante incidencias

ACTHO, establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la institución deberá comunicarlo, de manera inmediata, a los responsables de seguridad,

describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.

ACTHO, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos y debe incluirse como anexo en el presente manual.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

Evaluación y contención. Recibida la notificación, el Oficial de Protección de Datos Personales, con el apoyo del área o proveedor de tecnología, adoptará las medidas de contención, evaluará la naturaleza del incidente, las bases de datos y categorías de datos afectadas, el número aproximado de Titulares y el riesgo para sus derechos.

Reporte a la Superintendencia de Industria y Comercio. Cuando se presente una violación de los códigos de seguridad o existan riesgos en la administración de la información de los Titulares, ACTHO reportará el incidente a la SIC a través del RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecte y sea puesto en conocimiento del Oficial de Protección de Datos Personales (arts. 17 lit. n y 18 lit. k de la LEPD y Título V de la Circular Única de la SIC).

Comunicación a los Titulares. Cuando el incidente pueda afectar los derechos de los Titulares, ACTHO les informará sin dilaciones injustificadas la naturaleza del incidente, los datos comprometidos, las medidas adoptadas y las recomendaciones para mitigar sus efectos.

Cierre y lecciones aprendidas. Todo incidente se documentará en el registro de incidencias con las causas, las medidas correctivas y las acciones para evitar su repetición.

12.2 Reporte

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por ACTHO. Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el responsable de la información debe ser notificado de forma inmediata. Los colaboradores deben reportar a su jefe directo y/o al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de ACTHO. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún colaborador debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad, el asesor jurídico de ACTHO deberá intervenir con el fin de prestar el asesoramiento adecuado.

El responsable de la información debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, con el apoyo del área o proveedor de tecnología de ACTHO.

13. CONTROL DE ACCESO Y VIDEO VIGILANCIA

Control acceso: Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.

14. Medidas para el transporte, destrucción y reutilización de documentos y soportes.

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Antes de iniciar la destrucción se realizará un acta o se llevará el registro en un libro o agenda, en dicha notación se describirá el documento objeto de destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

 Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 45
--	---	-----------------------------------

15. Infracciones y sanciones

De acuerdo con el Capítulo II de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio puede imponer sanciones por el incumplimiento de la normativa sobre protección de datos al responsable del tratamiento o al encargado del tratamiento. Las posibles sanciones son:

Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

El incumplimiento de este manual por parte de los colaboradores de ACTHO será sancionado conforme al Reglamento Interno de Trabajo y al respectivo contrato; en el caso de contratistas y encargados, conforme a lo pactado en los contratos respectivos.

16. Vigencia

Las bases de datos responsabilidad de ACTHO, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. ACTHO, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Los plazos de conservación de cada base de datos son los siguientes:

- Proveedores: durante la relación contractual y hasta diez (10) años después de su terminación, por el deber de conservar los soportes contables (art. 28 de la Ley 962 de 2005).
- Clientes o asociados: durante la afiliación o la relación y hasta 5 años después de su terminación; los soportes contables y de facturación, diez (10) años. Los datos para finalidades comerciales se conservarán hasta que el Titular revoque la autorización.

 actho Asociación Colombiana de Talento Humano y Organizacional	Manual de políticas y procedimientos Habeas Data	Versión 4 Página 46
--	---	-----------------------------------

- Trabajadores: durante la relación laboral y, después de su terminación, por el tiempo necesario para atender obligaciones laborales, pensionales y de seguridad social por un plazo de 90 años.
- Aspirantes no seleccionados: hasta seis meses después de finalizado el proceso de selección, salvo que autoricen su conservación para futuras vacantes.
- Registros de acceso a sistemas: dos (2) años.
- Prueba de las autorizaciones y de la atención de consultas y reclamos: mientras dure el tratamiento y el término adicional necesario para atender reclamaciones o requerimientos de autoridad.