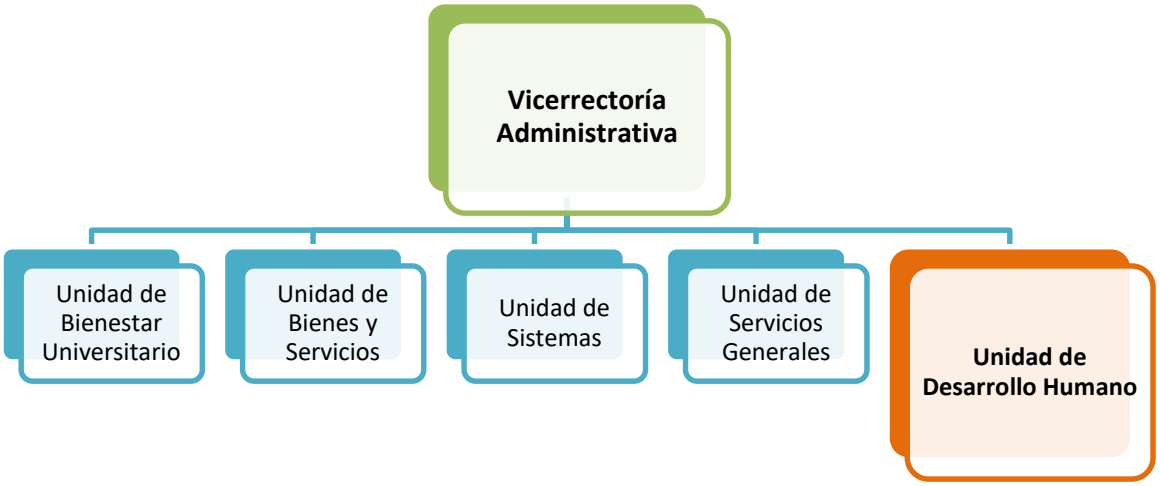
E.5.1. LINEAMIENTO INSTITUCIONAL PARA EL MANEJO DE DATOS PERSONALES EN EL PROCESO DE GESTIÓN DEL TALENTO HUMANO

El objetivo de este documento es ser utilizado como una herramienta para verificar el correcto tratamiento de datos personales en el proceso de gestión del talento humano cuya operación está, en principio, a cargo de la Unidad de Desarrollo Humano de **LA INSTITUCIÓN UNIVERSITARIA**, por esta razón, en el contenido de este documento se precisan los asuntos que son relevantes para la implementación y cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, con el fin de garantizarle a todos los titulares de datos de carácter personal su derecho fundamental de decidir sobre el uso y destino de los mismos, así como garantizar un tratamiento adecuado e impedir que se vulnere la intimidad y privacidad de los titulares de esta información.

Es necesario tener en cuenta, que la Vicerrectoría Administrativa de **LA INSTITUCIÓN UNIVERSITARIA** comprende las siguientes unidades:



La Unidad de Desarrollo Humano hace parte de la Vicerrectoría Académica, y es responsable de gestionar el talento humano de **LA INSTITUCIÓN UNIVERSITARIA** a través de la vinculación y selección de personal, la ejecución de los programas de capacitación, bienestar laboral e incentivos, la seguridad y salud en el trabajo, la implementación y seguimiento de la evaluación del desempeño de los funcionarios, buscando liderar procesos de cambio que fortalezcan las competencias y habilidades de los funcionarios y su sentido de pertenencia con la Institución.

Con todo, será necesario hacer referencia a los procesos de la Unidad de Desarrollo Humano, por cuanto en cada uno de estos se tratan datos personales, lo cual requiere tener absoluta claridad

de los riesgos asociados al mismo para poder establecer mecanismos adecuados para mitigarlos o reducir su impacto.

Para los efectos del presente lineamiento institucional, independiente del régimen legal o reglamentario aplicable a los servidores públicos, empleados de carrera administrativa o de libre nombramiento y remoción vinculados con **LA INSTITUCIÓN UNIVERSITARIA**, de acuerdo a lo contemplado en el Manual de Funciones, Competencias Laborales, Requisitos Mínimos para los niveles jerárquicos y empleos que conforman la Planta de Personal de la Institución, serán denominados genéricamente funcionarios.

En el presente documento se establecen las condiciones y requisitos mínimos para el debido manejo y custodia de los archivos y bases de datos que contengan información de carácter personal.

Para su mayor entendimiento, este documento se divide en ocho (8) partes así:

1. Elementos que permiten identificar un dato de carácter personal.
2. Definiciones Claves.
3. Derechos de los titulares de los datos de carácter personal.
4. Procesos de Desarrollo Humano de **LA INSTITUCIÓN UNIVERSITARIA** y recomendaciones específicas de cumplimiento.
5. Guía de procedimiento para la contratación de funcionarios.
6. Medidas de control frente a las tecnologías de la información en materia de subordinación.
7. Confidencialidad de la información en el marco de la relación administrativa – laboral.
8. Guía de procedimiento de gestión de archivo.

1. ELEMENTOS QUE PERMITEN IDENTIFICAR UN DATO DE CARÁCTER PERSONAL.

Con el fin de ayudar a determinar si la información que posee un área de **LA INSTITUCIÓN UNIVERSITARIA** es un dato personal, deberán tenerse en cuenta los siguientes elementos:

1.1. Que los datos sean referidos a aspectos exclusivos y propios de una persona natural.
1.2. Que permita identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos.
1.3. Que su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita.

1.4. El tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración, custodia, uso y divulgación.
1.5. Que la información se encuentre contenida en sus archivos o bases de datos propias.
1.6. Los datos pueden ser de cualquier tipo, una foto, un archivo de vídeo o sonido, numéricos, textos, etc.

2. DEFINICIONES CLAVES.

Con el objetivo de ayudar a determinar de una forma sencilla el significado del vocablo técnico utilizado frecuentemente en materia de protección de datos personales, todas las áreas de **LA INSTITUCIÓN UNIVERSITARIA** deberán entender los siguientes términos así:

2.1. Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
2.2. Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.
2.3. Consentimiento del titular: Es una manifestación de la voluntad, informada, libre e inequívoca, a través de la cual el titular de los datos de carácter personal acepta que un tercero utilice su información con fines comerciales.
2.4. Consultas: Los titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado.
2.5. Datos de carácter personal: Se refiere a la información de las personas naturales, relativa tanto a su identidad como a su existencia y ocupaciones.
2.6. Encargado del tratamiento: Es quien manipula los datos de carácter personal, pero no decide cómo, ni con qué fin. Su trabajo es operativo y se hace con base a las indicaciones e instrucciones del responsable del tratamiento.
2.7. Finalidad: La finalidad corresponde a los fines exclusivos para los cuales fue entregada por el titular. Se deberá informar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada, Cualquier utilización diversa, deberá ser autorizada en forma expresa por el Titular.
2.8. Habeas data: Es el derecho que todo titular de información tiene de conocer, actualizar, rectificar u oponerse a la información concerniente a sus datos personales. El habeas data confiere un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información. En este sentido este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático.
2.9. Protección de datos de carácter personal: Es un derecho fundamental que tienen todas las personas naturales. Busca la protección de su intimidad y privacidad frente a una

posible vulneración por el tratamiento indebido de datos personales capturados por un tercero.

2.10. **Reclamo:** El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley

2.11. **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.

2.12. **Sistema de información:** Conjunto de elementos orientados al tratamiento y administración de datos e información organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

2.13. **Tratamiento**: Cualquier operación o procedimientos físicos o automatizados que permita captar, registrar, reproducir, conservar, organizar, modificar, transmitir los datos de carácter personal.

2.14. **Titular de los datos personales:** Es la persona natural cuyos datos personales son objeto de tratamiento por parte de un tercero.

3. DERECHOS DE LOS TITULARES DE DATOS DE CARÁCTER PERSONAL.

El derecho de *habeas data* otorga un grupo de facultades a los titulares de información de carácter personal con el fin de controlar los datos que de esta persona se encuentran en un banco o base de datos y por otro lado para permitir controlar el flujo de sus datos que de esta persona se pueda dar; este grupo de facultades constituye en sí el núcleo esencial del derecho de habeas data los cuales son: **3.1.** Derecho de acceso; **3.2.** Derecho de rectificación; **3.3.** Derecho de cancelación; **3.4.** Derecho de oposición.

A continuación, se definirán cada uno de estos derechos de tal forma que cada área o dependencia de **LA INSTITUCIÓN UNIVERSITARIA** deberá entender por los mismos lo siguiente:

3.1. **Derecho de acceso:** Es el derecho que tiene todo titular de información de carácter personal para conocer los datos personales que figuren en un archivo o base de datos sometidos a tratamiento, determinando su origen, y qué posibles transmisiones o transferencias se han realizado o se prevean realizar en el futuro por parte de responsable del tratamiento.

3.2. **Derecho de rectificación:** El titular de los datos podrá solicitar al responsable del tratamiento la rectificación de sus datos personales cuando éstos sean inadecuados, incompletos, inexactos o excesivos.

3.3. **Derecho de cancelación:** Cuando el titular de los datos pueda tener conocimiento que sus datos personales que están siendo tratado por parte de la **CLÍNICA SIGMA** son inexactos o incompletos, inadecuados o excesivos, podrá solicitar de la cancelación de los mismos.

3.4. **Derecho de oposición:** En aquellos casos en que el consentimiento del titular para el tratamiento de sus datos no resulte necesario, éste podrá oponerse a dicho tratamiento cuando existan motivos fundados y legítimos.

4. PROCESOS DE LA UNIDAD DE DESARROLLO HUMANO EN LA INSTITUCIÓN UNIVERSITARIA Y RECOMENDACIONES ESPECÍFICAS DE CUMPLIMIENTO.

Como se precisó al inicio de este documento, la Unidad de Desarrollo Humano de **LA INSTITUCIÓN UNIVERSITARIA** comprende varios procesos, sobre los cuales a continuación se realizan algunas recomendaciones puntuales de cara al cumplimiento de la legislación nacional de protección de datos personales:

PROCESO	DESCRIPCIÓN Y RECOMENDACIONES
RECLUTAMIENTO Y SELECCIÓN	Respecto del tratamiento de los datos personales durante el proceso de reclutamiento y selección de personal, es importante advertir que es uno de los más críticos identificados en la etapa de entrevistas con los profesionales de la Unidad de Desarrollo Humano y levantamiento de información, debido a la gran cantidad de información personal, incluso sensible, que gestionan y almacenan como parte del proceso. En específico, se recomienda: • Limitar, en la medida de lo posible, las fuentes de reclutamiento a aquellas en las cuales puedan garantizar obtener la autorización para el tratamiento de los datos personales de los candidatos y les permita mitigar el riesgo del acceso de terceros no autorizados o uso inadecuado de la información de las hojas de

	vida. • Establecer un tiempo de retención de las hojas de vida de los candidatos a una vacante por un tiempo definido y descartar la de aquellos que no hayan sido seleccionados o no vayan a ser tenidos en cuenta. • Suscribir acuerdos de confidencialidad y de trasmisión de datos personales con todas las fuentes de reclutamiento externas que utilicen, cuando sea **LA INSTITUCIÓN UNIVERSITARIA** quien directamente los contrate. • Suscribir contratos de transmisión de datos personales con los contratistas – profesionales que en razón de su vínculo contractual deban acceder a información que contenga datos personales de cualquiera de los grupos de interés de **LA INSTITUCIÓN UNIVERSITARIA**. • Inventariar las bases de datos que contengan información personal que se gestionan en este proceso y suprimir toda aquella información que no sea necesaria o se esté utilizando actualmente, salvo que realmente se precise para atender algún requerimiento de autoridades judiciales o administrativas. • Implementar formatos de autorización para el tratamiento de datos personales desde el inicio del proceso de reclutamiento contemplando todas las finalidades requeridas en el mismo, el cual deberá adjuntarse al acta de nombramiento y posesión del cargo del funcionario que corresponda.
DESARROLLO HUMANO, BIENESTAR Y SALUD LABORAL	Este proceso gestiona información personal de los funcionarios en el aplicativo ÁRTICO para al pago de nómina, prestaciones sociales, parafiscales, seguridad social, entre otros. Se recomienda suscribir contratos de transmisión de datos personales con los bancos con los cuales se tiene convenio con relación a las aprobaciones de libranzas y pagos de libranzas o incluir cláusula de protección de datos personales vía otrosí en los contratos suscritos con estos contratistas, ya que se comparte información tal como el

	nombre, cédula, salario, descuentos que se le hacen a los funcionarios, y la fecha de terminación del contrato. Se recomienda mantener actualizada la información contenida en las bases de datos identificadas en la etapa de levantamiento de información, incluido el número de titulares.
SEGURIDAD Y SALUD EN EL TRABAJO	En este proceso se gestiona información sensible de los funcionarios y contratistas relacionada con su estado de salud y se identificaron varias bases de datos relacionadas con el SG-SST. Sobre la información almacenada en estas bases de datos, es importante mencionar que la misma es de carácter sensible, razón por la cual deben implementarse mayores medidas de seguridad que garanticen la confidencialidad, acceso y circulación restringida y conservación de la misma. A continuación se hacen algunas recomendaciones puntuales: • Los registros y documentos que soportan el Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST deben conservarse de manera controlada, garantizando que sean legibles, fácilmente identificables y accesibles, protegidos contra daño, deterioro o pérdida. • El responsable del SG-SST y la realización de las pruebas de riesgo psicosocial puede tener acceso a todos los documentos y registros exceptuando el acceso a las historias clínicas ocupacionales de los funcionarios cuando no tenga el perfil de profesional de salud especialista en seguridad y salud en el trabajo. • La conservación de estos documentos puede hacerse de forma electrónica de conformidad con lo establecido en el artículo 2.2.4.6.13. del Decreto 1072 de 2015, siempre y cuando se garantice la preservación de la información. • Restringir el acceso a la base de datos de evolución clínica del funcionario a un profesional médico o, en su

	defecto, suprimir el uso de esta base de datos.

5. GUÍA DE PROCEDIMIENTO PARA EL RECLUTAMIENTO Y SELECCIÓN DE PERSONAL.

Los procesos que se deben desarrollar al interior del área son, entre otros: proceso de reclutamiento y selección de personal, entrevista presencial, procedimiento de inducción y reinducción de funcionarios, procesos disciplinarios, actualización de datos, desvinculación laboral e implementación y seguimiento de la evaluación del desempeño de los funcionarios, buscando liderar procesos de cambio que fortalezcan las competencias y habilidades de estos.

5.1 Proceso de Reclutamiento y Selección de Personal: A continuación, las recomendaciones que se deben tener en cuenta al documentar el procedimiento para la vinculación de personal:

5.1.1 Reclutamiento: En el proceso de reclutamiento se incluyen por lo menos cinco (5) actividades en las que se involucra el tratamiento de datos personales.

5.1.2 Recepción de hojas de vida de aspirantes: Las hojas de vida de candidatos a vacantes que se entreguen de manera física o electrónica a la Unidad de Desarrollo Humano, ya sea porque las mismas han sido aportadas directamente por el candidato y/o referidas por un tercero, deben ser custodiadas por el responsable que haya asignado el director del área.

Cuando se trate de hojas de vida físicas, deberán archivarse en una carpeta especial, la cual deberá estar ubicada en un compartimento específico de la Unidad de Gestión Humana, en el centro de acopio o en las oficinas donde se reciban las mismas, las cuales deberán permanecer bajo llave y ser administrada por la persona encargada.

La recepción de las hojas de vida, sin excepción alguna, deberá contar con un acuse de recibo, en el que se deberá incorporar información sobre las finalidades de tratamiento y la remisión a la Política de Protección de Datos Personales.

5.1.3 Formato de impreso para entregar a los aspirantes: Se recomienda incluir en el Formato Único de Hoja de Vida o en un formato anexo el texto de autorización para el tratamiento de datos personales de los aspirantes. En dichos formatos deberá informar de forma plena la calidad de responsable que asumirá **LA INSTITUCIÓN UNIVERSITARIA** frente a los datos personales de los candidatos y garantizar el derecho de *Habeas Data* de los mismos.

5.1.4 Consulta en centrales de riesgos y bases de datos de la Contraloría y Procuraduría: Las consultas en las centrales de riesgo y antecedentes que se realicen sobre los candidatos a

una vacante de la empresa deberán contar siempre con la autorización del candidato como titular de datos personales y dentro de la misma deberá quedar claro que el resultado de dicha consulta será valorada con los elementos de juicio que técnicamente inciden en la referida finalidad y advertir que **LA INSTITUCIÓN UNIVERSITARIA** no se basará exclusivamente en la información relativa al incumplimiento de obligaciones financieras del aspirante para tomar una decisión sobre la contratación.

5.1.5. Destrucción de soporte: Una vez concluido este proceso de reclutamiento y se haya seleccionado a un candidato para ser vinculado a **LA INSTITUCIÓN UNIVERSITARIA**, los documentos físicos de los otros candidatos deberán ser destruidos y podrán conservarse en medio magnético por máximo cuatro (4) meses por si se requiere contar nuevamente con su información para efecto de una nueva posibilidad de vinculación. Los archivos físicos deberán destruirse, preferiblemente, en una máquina destructora de papel y bajo ninguna circunstancia podrán ser utilizados como papel reciclable.

Los documentos digitales, deberán ser eliminados del correo electrónico y del computador, tanto de la carpeta de archivo como de la papelera de reciclaje, de la bandeja de entrada del correo electrónico donde se recibió y de la papelera del mismo correo electrónico.

De igual manera, los documentos que han soportado las diferentes etapas en las que haya participado el candidato, tales como formato de aspirante, soportes de entrevistas, pruebas psicotécnicas y/o prácticas, formato de visita domiciliaria y valoración global del candidato, deberán destruirse de igual manera que las hojas de vida y, bajo ninguna circunstancia, este material podrá ser reutilizado como papel reciclable.

5.1.6. Vinculación del personal: Una vez seleccionado el candidato para formalizar el vínculo administrativo-laboral deberá firmar el acta de posesión con las cláusulas adicionales que recomendamos, las cuales comprenden (i) autorizaciones para el tratamiento de datos personales, (ii) autorización para el tratamiento de datos sensibles (datos relativos al estado de salud, historias clínicas, datos biométricos – huella – fotografía - videograbaciones), (iii) autorización para el tratamiento de los datos personales de los hijos menores de edad y la cesión de imagen propia y voz; (iv) uso exclusivo de herramientas tecnológicas; (v) reglas de uso de medios de comunicación, técnicos o tecnológicos, (vi) confidencialidad, (vii) reserva de la información, (viii) protección a la propiedad intelectual y derechos de autor.

**Las cláusulas mencionadas se encuentran en el documento denominado Formatos de Autorización y Cláusulas para incluir en el contratos de prestación de servicios de LA INSTITUCIÓN UNIVERSITARIA.*

Igualmente, recomendamos que se formalice el formato de autorización de datos personales para funcionarios, pues en éste se incluyen las finalidades del tratamiento de la información personal para la relación administrativa-laboral entre las partes, se autoriza el tratamiento de datos de carácter sensible, autoriza el eventual tratamiento de la información de sus hijos menores de edad (si los tiene) y queda plenamente determinado que se le ha informado los derechos que les asisten como titulares de datos personales y los canales habilitados por **LA INSTITUCIÓN UNIVERSITARIA** para su ejercicio.

5.2. Inducción al personal: Deberá incluir capacitación e información sobre el tratamiento de datos personales en la organización, la cual puede ser dictada por el delegado u oficial de protección de datos personales que la Vicerrectora Administrativa haya designado para dicho efecto. Para realizar esta sensibilización, la persona encargada podrá compartir el instructivo en materia de protección de datos personales entregado como de soporte de capacitaciones e igualmente deberá socializarle el aviso de privacidad y política de tratamiento de la información de **LA INSTITUCIÓN UNIVERSITARIA.**

5.3. Proceso disciplinario: Cuando se lleve a cabo un proceso disciplinario con un funcionario, el mismo debe efectuarse conforme a lo estipulado en las resoluciones internas y los documentos relacionados con este proceso y deben ser custodiados por la persona encargada y archivados dentro de su expediente laboral, garantizando siempre su acceso y circulación restringida a terceros no autorizados.

En caso de que se realicen consultas sobre el estado de cumplimiento de las obligaciones y pasado judicial de los funcionarios de **LA INSTITUCIÓN UNIVERSITARIA** en centrales de riesgo crediticio y las bases de datos de la contraloría, procuraduría, es indispensable contar la debida autorización de dichos funcionarios y en la misma advertir que el resultado negativo de esta consulta será tenido en cuenta para el proceder de vinculación con la entidad.

5.4. Formato desvinculación laboral: En caso de realizarlo, deberá custodiarse el documento de paz y salvo junto con la entrevista de retiro de manera especial y confidencial, pues puede contener información sensible que pueda afectar al ex funcionario.

6. MEDIDAS DE CONTROL FRENTE A LAS TECNOLOGÍAS DE LA INFORMACIÓN EN MATERIA DE SUBORDINACIÓN.

Las medidas que se tomen y relacionen las tecnologías de la información sobre los subordinados (funcionarios) que pueda de alguna forma poner en peligro la intimidad o privacidad de estos, deberán ser comunicadas con el fin de cumplir con la normatividad vigente en materia de protección de datos personales.

Debe tenerse en cuenta que el uso de tecnologías de la información en materia de control de los funcionario para el cumplimiento de las obligaciones derivadas de relación administrativa-laboral, no podrán, en ningún momento, vulnerar el honor, la dignidad y sus derechos mínimos, tal como lo consagra nuestra constitución política que otorga especial protección al trabajo.

Cuando se trate de los datos personales aportados por el funcionario tal como lo indica la Sentencia C-748 de 2011 *"el que los datos no circulen o circulen internamente, no asegura que su tratamiento no pueda tener consecuencias adversas para su titular"*, es por eso que al establecerse medidas tecnológicas de control sobre los subordinados (funcionarios) que puedan poner en peligro la intimidad o privacidad de estos, deberán en todo momento ser comunicadas con el fin de cumplir con la normatividad vigente en materia de protección de datos personales. (Sentencias T-696 de 1996, T-405 del 2007 y C-1110 del 2001).

Es así como se puede afirmar que el uso de las tecnologías de la información como herramienta de control cuando se trata de dar cumplimiento a las obligaciones que emanan del contrato laboral, influyen, generalmente, en la intimidad y/o privacidad del funcionario, es por eso que se relacionan las medidas de control que actualmente se utilizan o podrían ser utilizadas por parte de **LA INSTITUCIÓN UNIVERSITARIA**, tales como: (i) Videovigilancia; (ii) Controles sobre el correo electrónico (análisis y monitoreo); y (iii) Biometría.

6.1. Videovigilancia: Será necesario disponer avisos de privacidad que le adviertan al funcionario que por motivos de seguridad se han instalado cámaras de video en las instalaciones e indicar en qué lugares están instaladas. De la misma manera, en dicho aviso se deberá advertir que las grabaciones producto del monitoreo formarán parte de la base de datos de **LA INSTITUCIÓN UNIVERSITARIA** y que una de sus finalidades será el control de acceso a las instalaciones y mantener la seguridad de las instalaciones. Se entrega como Anexo No. 1 el modelo de aviso de videovigilancia.

6.2. Correo Electrónico: Si se realizan monitorizaciones al correo electrónico de los funcionarios es necesario informarles de manera expresa y clara sobre dicha situación. Se recomienda dado el caso, dar a conocer la política que desarrolle **LA INSTITUCIÓN UNIVERSITARIA** en este

sentido. Se deberá describir y definir de forma detallada en qué medida los funcionarios pueden utilizar los sistemas de comunicación con los que cuente **LA INSTITUCIÓN UNIVERSITARIA**.

6.3. Datos Biométricos: Los datos biométricos son de carácter sensible, los cuales se refieren al reconocimiento biométrico, que indica que se trata de *métodos automatizados que pueden de manera precisa reconocer a un individuo con base en características físicas o de comportamiento (...),* y dentro de esta *tecnología reconocimiento de huellas digitales.*

Cuando se requiera utilizar la tecnología biométrica para realizar tratamiento de los datos de los funcionarios vinculados con **LA INSTITUCIÓN UNIVERSITARIA,** se debe tener claro que realizar este tratamiento implica una responsabilidad reforzada para la organización, por lo que es necesario contar siempre con el consentimiento explícito del titular de los datos.

Estos datos deben ser tratados conforme al principio de libertad, el cual *no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez,* es por esta razón que el responsable del tratamiento debe tener la autorización explícita del titular de los datos; autorización explícita que puede ser verbal, pero que deberá tener como probarla dada la connotación de responsabilidad reforzada que implica su tratamiento por tratarse de casos exceptuados que pueden generar alto riesgo de vulneración.

Cuando se trate del uso de un lector biométrico según el concepto No. 133248 del Ministerio de Trabajo de fecha 24 de Julio de 2015, en el cual se ratifica que en ningún aparte de las normas de vinculación de servidores públicos se evidencia alguna prohibición sobre el uso de datos biométricos de los funcionarios y se advierte, asimismo, que **LA INSTITUCIÓN UNIVERSITARIA** debe ceñirse estrictamente al manejo que de los mismos se establezca en el la Política de Tratamiento de Datos Personales de **LA INSTITUCIÓN UNIVERSITARIA**. Así las cosas, el tratamiento de datos biométricos del funcionario es permitido, pero tendrá un componente importante de desarrollo interno de autorregulación en **LA INSTITUCIÓN UNIVERSITARIA**, el cual comporta la implementación de un procedimiento interno para el tratamiento de este tipo de datos, hacer suscribir cláusulas de autorización en los términos previstos en la ley respecto del tratamiento de sus datos sensibles, vía formato de autorización explícita por parte del funcionario o vía otrosí a los contratos de prestación de servicios suscritos con los contratistas para el tratamiento de sus datos sensibles, específicamente el dato biométrico para el control de acceso a las instalaciones.

7. CONFIDENCIALIDAD DE LA INFORMACIÓN EN EL MARCO DE LA RELACIÓN LABORAL

Es importante determinar algunos puntos relacionados con las obligaciones de los funcionarios de **LA INSTITUCIÓN UNIVERSITARIA**, tales como, el deber de confidencialidad, tiempo de reserva Y custodia de la información por parte del funcionario después de finalizada la relación administrativa - laboral, para lo cual resaltaremos algunas consideraciones importantes.

En el marco jurídico colombiano, las normas que enmarcan la confidencialidad de la información conocida en razón a un contrato de trabajo se identifican como: (i) Ley 256 de 1996 (artículo 16 violación de secretos); (ii) Decisión 486 de 2000 (Artículo 262 Secretos Empresariales); (iii) Código Penal (Artículo 308 Violación de reserva industrial o comercial), (iv) Ley 909 de 2004, reglamentada parcialmente por el Decreto Nacional 4500 de 2005, Decreto 3905 de 2009, Decreto 4567 de 2011. 734 de 2002 y el Capítulo IV de la Ley 734 de 2002.

Para el caso de los empleados públicos y de carrera administrativa, conforme a la normatividad citada anteriormente, estos tendrán la obligación de no comunicar con terceros, salvo autorización expresa, las informaciones que tenga sobre sus funciones, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios a la entidad, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales del empleo público ante las autoridades competentes, sin embargo, una vez terminada la relación administrativa - laboral, nada dicen las normas sobre la obligación o no de guardar confidencialidad sobre la información conocida por un funcionario en relación a la actividad o labor desarrollada en virtud de vinculación administrativa – laboral con la entidad.

Quedará entonces bajo el arbitrio de **LA INSTITUCIÓN UNIVERSITARIA** un plazo sobre la obligación que tendrá el funcionario declarado insubsistente o desvinculado por razones del servicio de no revelar información que haya obtenido en relación a la actividad que este haya venido desarrollando en virtud de su nombramiento. Dicha condición puede pactarse desde el inicio de la relación administrativa - laboral, con la firma del acta de posesión, o de forma posterior a través de la suscripción de un documento que haga parte de su historia laboral.

Por lo anterior, independiente de que exista una obligación general de confidencialidad en el Manual de Funciones de la entidad, el funcionario tendrá la obligación de no comunicar con terceros información a la que tenga acceso por el vínculo creado con **LA INSTITUCIÓN UNIVERSITARIA**, sin embargo, es importante contemplar en la obligación de confidencialidad el tiempo durante el cual debe conservarse la información bajo reserva una vez terminada la relación legal o contractual. Esto aplica tanto para funcionarios como para aprendices, practicantes y pasantes.

Está firma consultora considera que debido a que la información es un activo valioso para **LA INSTITUCIÓN UNIVERSITARIA** la confidencialidad que debe estipularse una vez terminada la relación administrativa – laboral debe ser la más amplia posible, debido a que, durante el desarrollo de las actividades propias en este tipo de entidades, es normal que la entidad facilite información de todo tipo a su funcionario (incluido aprendiz y practicante) para el cumplimiento de sus obligaciones. Siempre existirá el riesgo sobre la pérdida de la información durante la relación administrativa - laboral, pero una vez terminada, el riesgo para la entidad se mantiene, e inclusive se puede incrementar debido a que el nivel de compromiso u obligación del funcionario declarado insubsistente o desvinculado de la entidad pública por razones del servicio se ha debilitado, e inclusive en muchas ocasiones desaparecido, dependiendo de situaciones relacionadas con la terminación de la relación administrativa - laboral.

El aspecto clave en la estipulación amplia del plazo de confidencialidad que deberá guardar el funcionario una vez se termine la relación administrativa – laboral, dependerá de cuestiones como el nivel de daño que pueda causarse al titular de la información que pueda ser potencialmente revelada. En muchas ocasiones la información que se considerada clasificada durante un determinado periodo, pierde dicha condición, convirtiéndose en información de carácter público, sobre la cual ya no será exigible la obligación de reserva o confidencialidad.

Lo anterior, sin perjuicio de lo establecido en la Ley 1712 de 2014 "*Ley Transparencia y Acceso a la Información Pública",* en virtud de la cual se establecen los límites admisibles al derecho de acceso a la información pública proveniente de la necesidad de la protección de otros derechos fundamentales que puedan ser afectados por el acceso y difusión de tal información. Tal es el caso de los datos personales que sólo pertenecen a su titular y cuya divulgación podría afectar un derecho legítimo de este último como el derecho a la intimidad, o de los secretos comerciales, industriales y profesionales, cuyo acceso puede afectar el ejercicio de las libertades económicas. También se ha autorizado restringir el acceso a la información pública cuando su divulgación o acceso pueda poner en peligro la vida, la integridad o seguridad de las personas. Las restricciones contenidas en el artículo 18 *sub-examine* tendrán una vigencia indefinida, pero no podrán aplicarse cuando la persona haya consentido en la revelación de esta información.

Al respecto, de conformidad con lo establecido en el artículo 74 de la Constitución Política y la jurisprudencia constitucional sobre la materia, una "*reserva legal sólo puede operar sobre la información que compromete derechos fundamentales o bienes constitucionales pero no sobre todo el proceso público dentro del cual dicha información se inserta. En ese sentido en un caso de violencia contra menores, por ejemplo, solo es reservado el nombre del menor o los datos que permitan su identificación, pero no el resto de la información que reposa en el proceso, pues resultaría desproporcionado reservar una información cuyo secreto no protege ningún bien o*

derecho constitucional. A este respecto no sobra recordar que la Corte ha señalado que cualquier decisión destinada a mantener en reserva determinada información debe ser motivada y que la interpretación de la norma sobre reserva debe ser restrictiva."[1]

Con todo, para contribuir en la definición de la discusión entre el acceso a la información pública o la protección de los datos personales, si los documentos públicos que contienen datos personales pueden divulgarse en su totalidad, si se divulgan los datos personales de un funcionario público que son necesarios para ejercer el control social de su gestión, o si se divulgan aquellos que se requieran para hacer una investigación o un estudio que sirva de soporte a un documento de política pública, debe aplicarse el artículo 28 de la Ley de Transparencia y Acceso a la Información Pública que, al ser la única norma que se plantea esta dificultad, resulta ser la guía hermenéutica más adecuada para atender la tensión entre el *habeas data* y el acceso a la información pública.

8. GUÍA DE PROCEDIMIENTO DE GESTIÓN DE ARCHIVO.

Es importante mencionar que **LA INSTITUCIÓN UNIVERSITARIA** tiene implementado actualmente un Programa de Gestión Documental (PGD) el cual tiene como objetivo *"poner a disposición estrategias y métodos que permitan el control de las actividades administrativas y técnicas tendientes a la planificación, manejo, organización y conservación del documento desde su origen hasta su destino final, independiente del soporte en que se encuentre (análoga o digital), garantizando la eficiencia de la Gestión y la conservación del patrimonio documental."*

Con la ejecución del Programa de Gestión Documental se logra la racionalización y control de la producción documental en atención a los procedimientos administrativos, flujos documentales, implementación de modelos y formatos para el registro de documentos, materiales soportes y equipos de calidad que faciliten la preservación y el cuidado del medio ambiente, la normalización del Procedimiento IG.2.19.2.07 Recepción, Distribución y Trámite de Comunicaciones Oficiales y la regulación de la gestión documental mediante la aplicación de la Tabla de Retención Documental.

Elaborar un procedimiento para la gestión de la información de los funcionarios facilita el manejo de información que en muchas ocasiones puede resultar sensible o crítica para el funcionario, con las consecuencias legales que ello implica para el responsable del tratamiento, en este caso **LA INSTITUCIÓN UNIVERSITARIA.**

A continuación, presentamos una guía para ajustar, si a ello hay lugar, el procedimiento recomendado:

[1] Corte Constitucional. Sentencia C-274 de 2013. M.P. María Victoria Calle.

8.1. GENERALIDADES:

En este punto se definen los objetivos, el alcance, gestión de la información y clasificación de los datos que se tratan en la Unidad de Desarrollo Humano. La historia laboral[2] deberá siempre estar actualizada so pena de incumplimiento a lo establecido en la Ley 1581 del 2012.

8.1.5. Objetivo: Proteger y controlar la conservación y custodia de la información que se recibe y se generen en la Unidad de Desarrollo Humano de **LA INSTITUCIÓN UNIVERSITARIA.**

8.1.6. Alcance: Aplica para todos los documentos recibidos y generados por la Dirección de Gestión Humana de **LA INSTITUCIÓN UNIVERSITARIA** entendidos estos como los que surgen de los procesos de reclutamiento, selección, vinculación y desvinculación del personal contratado por dicha entidad.

8.1.7. Archivo de gestión: Comprende toda la documentación que es sometida a permanente utilización y consulta administrativa por la Unidad de Desarrollo Humano y demás departamentos que los soliciten en cabeza del jefe del área.

8.2. NORMAS DE ARCHIVO DE DESARROLLO HUMANO.

A continuación se relacionan las principales normas de archivo aplicables a los distintos procesos de la Unidad de Desarrollo Humano:

CONCEPTO	NORMA	CONTENIDO
		Artículo 2.2.4.6.13. Conservación de los documentos. El empleador debe conservar los registros y documentos que soportan el Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST de manera controlada, garantizando que sean legibles, fácilmente identificables y accesibles, protegidos contra daño, deterioro o pérdida. El responsable del SG-SST tendrá acceso a todos los documentos y registros exceptuando el acceso a las historias clínicas ocupacionales de los funcionarios cuando no tenga

2 Sentencia T-592/13. HISTORIA LABORAL -Contenido y finalidad. En el caso particular de la historia laboral, la Corte ha establecido que la información que la compone, por ejemplo, tiempo de servicio, salario devengado, cotizaciones a la seguridad social, vacaciones disfrutadas, consignación de cesantías, ascensos, licencias, entre otros, es indispensable para acceder al goce efectivo de las prestaciones sociales en cabeza del funcionario. Por lo anterior es necesario que la información laboral contenida en los archivos sea veraz, cierta, clara, precisa y completa "a fin de que, de un lado, el funcionario pueda reclamar los derechos que le asisten, y, del otro, se protejan en su integridad los demás derechos fundamentales de los que son titulares."

Seguridad y Salud en el Trabajo (SGSST)	**Decreto 1072 de 2015**	perfil de médico especialista en seguridad y salud en el trabajo. La conservación puede hacerse de forma electrónica de conformidad con lo establecido en el presente decreto siempre y cuando se garantice la preservación de la información. Los siguientes documentos y registros, deben ser conservados por un periodo mínimo de veinte (20) años, contados a partir del momento en que cese la relación administrativa - laboral del funcionario con la empresa: **1.** Los resultados de los perfiles epidemiológicos de salud de los funcionarios, así como los conceptos de los exámenes de ingreso, periódicos y de retiro de los funcionarios, en caso que no cuente con los servicios de médico especialista en áreas afines a la seguridad y salud en el trabajo; **2.** Cuando la empresa cuente con médico especialista en áreas afines a la seguridad y salud en el trabajo, los resultados de exámenes de ingreso, periódicos y de egreso, así como los resultados de los exámenes complementarios tales como paraclínicos, pruebas de monitoreo biológico, audiometrías, espirometrías, radiografías de tórax y en general, las que se realicen con el objeto de monitorear los efectos hacia la salud de la exposición a peligros y riesgos; cuya reserva y custodia está a cargo del médico correspondiente; **3.** Resultados de mediciones y monitoreo a los ambientes de trabajo, como resultado de los programas de vigilancia y control de los peligros y riesgos en seguridad y salud en el trabajo; **4.** Registros de las actividades de capacitación, formación y entrenamiento en seguridad y salud en el trabajo; y,

		5. Registro del suministro de elementos y equipos de protección personal. Para los demás documentos y registros, el empleador deberá elaborar y cumplir con un sistema de archivo o retención documental, según aplique, acorde con la normatividad vigente y las políticas de la empresa.
HISTORIA LABORAL	**Sentencia T-926 de 2013**	La historia laboral, para la compone, por ejemplo, tiempo de servicio, salario devengado, cotizaciones a la seguridad social, vacaciones disfrutadas, consignación de cesantías, ascensos, licencias, entre otros, es indispensable para acceder al goce efectivo de las prestaciones sociales en cabeza del funcionario. Por lo anterior es necesario que la información laboral está contenida en archivos de manera veraz, cierta, clara, precisa y completa "*a fin de que, de un lado, el funcionario pueda reclamar los derechos que le asisten, y, del otro, se protejan en su integridad los demás derechos fundamentales de los que son titulares.* En este orden de ideas, debe resaltarse la importancia de que el acopio y la conservación de información se hagan con sujeción a los principios del *habeas data* con el fin de garantizar su integridad y veracidad y así salvaguardar los demás derechos de los titulares de la información. Con frecuencia esta información es necesaria para acceder al goce efectivo de otros derechos fundamentales, toda vez que los datos personales, laborales, médicos, financieros y de otra índole que están contenidos en archivos y bases de datos, son la fuente de la información que se utiliza para evaluar el cumplimiento de los requisitos para el reconocimiento de derechos y prestaciones.

HISTORIA LABORAL	**Sentencia T-079 de 2016**	Las obligaciones que la ley y la jurisprudencia les han atribuido a las administradoras de los regímenes pensionales respecto del manejo de la información y de los soportes que acreditan las cotizaciones efectuadas por sus afiliados desarrollan cada una de las perspectivas expuestas: la de la historia laboral como soporte probatorio del esfuerzo económico realizado por el funcionario para acceder a los ingresos que no podrá procurarse por sí mismo en cierta etapa de su vida y la de la historia laboral como documento contentivo de datos personales que requieren de un tratamiento especial , consecuente con la entidad de los bienes jurídicos involucrados en el manejo de la información que consignan.
	Código Sustantivo del Trabajo	**ARTÍCULO 264. ARCHIVOS DE LAS EMPRESAS.** Las empresas obligadas al pago de la jubilación deben conservar en sus archivos los datos que permitan establecer de manera precisa el tiempo de servicio de sus funcionarios y los salarios devengados.
VACACIONES	**Concepto 164331 de 01-06-2009**	Todo empleador debe llevar un registro especial de vacaciones en que el anotará la fecha en que ha ingresado al establecimiento cada funcionario, la fecha en que toma sus vacaciones anuales y en que las termina y la remuneración recibida por las mismas (Art. 187 C.S.T.)
TRABAJO SUPLEMENTARIO	**Código Sustantivo del Trabajo**	**ARTÍCULO 162.** El empleador está obligado a entregar al funcionario una relación de horas extras laboradas, con las mismas especificaciones anotadas en el libro de registro.

8.3. GESTIÓN DOCUMENTAL EN LA UNIDAD DE DESARROLLO HUMANO.

8.3.5. La Unidad de Atención al Ciudadano y de Archivo es responsable de los procesos archivísticos de los documentos a su cargo, desde su producción o recepción, hasta su disposición final, salvaguardando el patrimonio documental de la Institución mediante la implementación de planes y procedimientos consecuentes con las normas vigentes en temas archivísticos.

8.3.6. Los documentos del archivo de gestión en la Unidad de Desarrollo Humano deben guardarse en adecuadas unidades de conservación y almacenamiento, debidamente marcados, sin exposición a humedad, polvo o agentes biológicos que puedan deteriorarlos.

8.3.7. Los documentos en custodia deberán almacenarse en carpetas debidamente marcadas o rotuladas. Se respetará el nombre asignado al documento en todas las etapas, tales como archivo en gestión, archivo inactivo e histórico, si es del caso.

8.3.8. Debe existir acceso restringido al lugar donde se almacena la información de tipo personal para que se impida o evade el acceso de personas no autorizadas.

8.3.9. Los archivadores, armarios u otros anaqueles ubicados en el área deberán estar protegidos con llave u otra medida de seguridad que asegure que no se permitirá un acceso no autorizado.

8.3.10. Los documentos de carácter confidencial se encontrarán debidamente almacenados en estantes con acceso restringido y con llave.

8.3.11. La documentación que sean archivados deberá estar en buen estado, completamente depurados, seleccionados, limpios y ser claramente identificable.

8.3.12. La consulta de los archivos referentes al reclutamiento, selección, vinculación, hojas de vida del funcionario actual y desvinculación, solo podrá ser autorizada por el líder de la Unidad de Desarrollo Humano o quien haga sus veces.

8.3.13. Se recomienda establecer la custodia de las hojas de vida para procesos de reclutamiento podrán permanecer en custodia de **LA INSTITUCIÓN UNIVERSITARIA** por el periodo máximo de cuatro (4) meses, una vez finalizado este periodo y no haber sido elegidas para iniciar un proceso de selección, las mismas deberán ser destruidas en un medio idóneo para garantizar que estos documentos no sean reutilizados por ninguna persona al interior de la compañía o algún tercero externo. Es claro que estos documentos bajo ninguna circunstancia podrán ser utilizados como papel reciclable para otros fines diferentes a los cuales fueron recibidos.

8.3.14. Cuando el archivo o paquete de información del aspirante, junto con sus anexos, entendidos como pre entrevista, entrevista, pruebas, visitas domiciliarias, autorizaciones y demás, no es seleccionado en el proceso de selección, esta deberá ser destruida en el periodo máximo de un (1) año contados a partir de su la terminación de dicho proceso de

selección. Su destrucción debe ser a través en un medio idóneo para garantizar que estos documentos no sean reutilizados por ninguna persona al interior de la compañía o algún tercero externo. Es claro que estos documentos bajo ninguna circunstancia podrán ser utilizados como papel reutilizado para otros fines diferentes a los cuales fueron recibidos.

8.3.15. La información de la historia del funcionario debe ser custodiada por una sola dependencia o área con medidas de seguridad que permitan establecer controles sobre el acceso a la misma.

8.3.16. Deberá adoptarse un protocolo de autorizaciones del área para tener claridad que funcionario puede acceder a la información almacenada.

8.3.17. Se recomienda no incorporar datos personales de carácter sensible a la carpeta de los funcionarios, más allá de los que puedan llegar a ser necesarios para la gestión del contrato.

8.3.18. En caso de que se recopile información de tipo sensible, la misma deberá separarse y no deberá ser accesible por personas no autorizadas ya que la divulgación de este tipo de información al interior de **LA INSTITUCIÓN UNIVERSITARIA** puede generar discriminación y acoso al funcionario afectado.

8.3.19. Procurar por la disminución de la impresión de documentos, haciendo uso apropiado de los medios electrónicos y evitando la duplicidad necesaria de la información.

8.3.20. Los documentos de carácter confidencial o que contengan información de tipo personal ya sea del personal vinculado o en proceso de reclutamiento o selección no podrá ser utilizado como “papel reciclable”, estos documentos deberán ser destruidos con los medios idóneos para garantizar que los mismo no sean reutilizados por ninguna persona al interior de la compañía o algún tercero externo.

8.3.21. Cuando se determine la eliminación de archivos o destrucción de los mismos, se deberá destruir de manera tal que impida su recuperación, podrá realizarse a través de una máquina destructora de papel.

8.3.22. Cuando se trate de información de embargos o desembargos de un funcionario como parte de un proceso judicial en el que este hace parte, la información deberá ser manejada estrictamente entre el funcionario y el encargado del proceso. Bajo ninguna circunstancia la información de este proceso podrá permanecer en los escritorios o quedar expuesta a que un tercero u otro funcionario de la empresa pueda acceder, visualizar o utilizar la misma sin la debida autorización.

*****FIN DEL DOCUMENTO*****

En cumplimiento de la ley estatutaria 1581 de 2012 y sus decretos reglamentarios, se informa a visitantes, empleados, contratistas y proveedores que:

Con el fin de i) garantizar la seguridad de las instalaciones, de los bienes y de las personas y ii) verificar el cumplimiento de las obligaciones y los deberes de sus funcionarios, LA INSTITUCIÓN UNIVERSITARIA, identificada con el NIT. 805.001.868-0, se han instalado cámaras en distintas partes de sus instalaciones físicas para realizar el monitoreo y grabación de imágenes a través de un circuito cerrado de televisión (CCTV).

Las imágenes grabadas serán almacenadas en una base de datos de propiedad de LA INSTITUCIÓN UNIVERSITARIA, las cuales serán utilizadas para las finalidades arriba indicadas. Las imágenes serán suprimidas en un plazo máximo de [7] días. De igual forma, estos datos podrán ser suministrados a las fuerzas y cuerpos de seguridad del Estado, previa orden judicial o administrativa.

Usted como titular de datos personales podrá ejercer los derechos de acceso, rectificación, prueba de autorización, oposición y supresión, este último cuando no medie un deber legal o contractual que lo impida. Para dicho efecto, **LA INSTITUCIÓN UNIVERSITARIA** ha establecido los siguientes canales de contacto: i) **Correo electrónico**: atencionalciudadano@endeporte.edu.co, ii) **Dirección**: Calle 9 No. 34 – 01 y iii) **PBX**: (+572) [5540404].

Para mayor información sobre la Política de Tratamiento de Datos Personales o el Aviso de Privacidad de LA INSTITUCIÓN UNIVERSITARIA, puede consultarlas en el sitio web: http://www.endeporte.edu.co/