1. OBJETIVO

El presente documento tiene por objetivo recopilar las políticas en relación con la administración de los datos personales de **PEGSA LTDA (en adelante PEGSA)** y proteger el derecho de Habeas Data dando así cumplimiento a la ley 1581 de 2012 y a los decretos 1074 de 2013 y 886 de 2014 que garantizan el debido tratamiento conforme a la finalidad informada en la autorización dada.

2. ALCANCE

Dar cumplimiento a la normatividad colombiana vigente que protege el derecho de Habeas Data garantizándole a los titulares el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos personales, limitando a través de estas políticas y sus procedimientos las posibilidades de su divulgación, publicación o cesión.

Esta política se refiere a Datos Personales provenientes de personas naturales, cobijando a todos los empleados, clientes y proveedores de PEGSA, así como a los potenciales clientes o terceros con quienes la sociedad mantiene comunicación.

Dentro de la compañía NO hay Tratamiento de Datos Sensibles de los Titulares de los Datos Personales que trata la compañía, salvo en lo relacionados con los trabajadores.

3. ACLARACIÓN

Con el fin de conservar la estructura del Sistema de Gestión de Calidad de PEGSA se diseñaron un conjunto de tres documentos que conforman las Políticas y Procedimientos de Protección de Datos Personales y que han sido divididas de la siguiente manera: El GDO-PR-02 enfocado en las Políticas de Protección de Datos Personales, el GDO-PR-03 enfocado en los procedimientos de Protección de Datos Personales y el GDO-PR-04 enfocado en los riesgos asociados con la protección de los datos personales.

4. DEFINICIONES Y/O ABREVIATURAS.

Habeas Data: La Corte Constitucional lo definió como el derecho que otorga la facultad al titular de datos personales, de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información.

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

Base de Datos: Conjunto organizado manual o automático de datos personales que sea objeto de Tratamiento.

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

Dato sensible: Aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenecía 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, es decir que PEGSA le está encomendando el manejo de un compendio de datos personales, que sean entregados directamente por los titulares del dato o por terceros.

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.

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.

5. FINALIDAD DE TRATAMIENTO DE LOS DATOS

La información recolectada por PEGSA tiene como propósito permitir el adecuado desarrollo de su objeto social dentro del suministro de productos y servicios en el sector industrial y comercial, incluyendo el sector de los hidrocarburos y de generación de energía. Además, PEGSA guarda la información necesaria para dar cumplimiento a deberes legales, principalmente en materia contable, tributaria, societaria, y laboral.

La información sobre clientes, proveedores, socios y empleados, actuales o pasados, se guarda con el fin de facilitar, promover, permitir o mantener relaciones de carácter laboral, civil y comercial.

La información sobre actores del mercado de hidrocarburos y de generación de energía se almacena con el fin de dar cumplimiento a las actividades propias de su objeto social, particularmente las relacionadas con el desarrollo, planeación e implementación de proyectos, negocios, contratos o convenios comerciales. PEGSA recolectará los datos personales, como nombres, apellidos, dirección laboral, correo electrónico corporativo, y teléfono con el único propósito de usar y tratar los datos personales en el giro normal de sus negocios así:

Empleados: Procesos de reclutamiento y selección, elaboración del contrato de trabajo, pagos de nómina y seguridad social, afiliaciones y cumplimiento de la normatividad vigente, incluyendo los aspectos tributarios. De los empleados se recolecta como dato sensible la huella dactilar con los únicos propósitos de otorgar el acceso a las instalaciones de la compañía y los datos médicos de acuerdo con la normatividad laboral y la reglamentación HSEQ.

Clientes: Poder desarrollar negocios, ejecución de contratos y realizar el seguimiento a los diferentes proyectos que se realicen, estudio en listas restrictivas sobre lavado de activos y financiación al terrorismo, estudio de crédito, conocimiento del cliente, gestión de cobranza y reportes requeridos por las autoridades incluyendo los tributarios. Así como poder programar los mantenimientos de los equipos instalados. Estos datos personales podrán circular dentro de la compañía siempre y cuando sea para los fines anteriormente expuestos.

Proveedores: Poder desarrollar negocios, ejecución de contratos y realizar el seguimiento a los diferentes proyectos que se realicen, gestión de pagos, así como estudio en listas restrictivas sobre lavado de activos y financiación al terrorismo, reportes requeridos por las autoridades incluyendo los tributarios, poder programar los mantenimientos de los equipos instalados. Estos datos personales podrán circular dentro de la compañía siempre y cuando sea para los fines anteriormente expuestos.

Otros: Para llevar un control de la correspondencia, contestar la correspondencia recibida, personas que nos visitan, nos contactan o nos envían peticiones quejas y reclamos.

6. RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE LOS DATOS PERSONALES

El Responsable del Tratamiento de los datos personales es PEGSA, con domicilio en la ciudad de Bogotá. Los datos de contacto son los siguientes: Dirección oficinas: Transversal 55 #98ª-66 ofc 411 Centro Comercial Iserra 100, teléfono: 6210345 y Correo electrónico: datos.personales@pegsa.com.co

El Encargado es la persona natural o jurídica, pública o privada (empleados, clientes o proveedores), que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable.

De acuerdo a la norma, EL RESPONSABLE Del Tratamiento del dato personal, (PEGSA) y EL ENCARGADO del tratamiento, responden concurrente y solidariamente frente al titular del dato personal. Lo anterior frente a la veracidad, integridad, finalidad e incorporación del dato personal, así como en el tratamiento (uso, recolección, almacenamiento, circulación y supresión) del mismo; en el entendido que cualquier uso debe hacerse con autorización del titular.

7. DERECHOS DE LOS TITULARES

PEGSA informa a los Titulares de Datos Personales que los derechos que pueden ejercer de acuerdo con la Ley 1581 de 2012, son los siguientes:

- Conocer, actualizar y rectificar sus datos personales frente a PEGSA Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- 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 Ley 1581 de 2012.
- Ser informado por PEGSA. del Tratamiento, previa solicitud, respecto del uso que les ha dado a los datos personales del Titular.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
- Acceder en forma gratuita a sus Datos Personales que hayan sido objeto de Tratamiento.

8. LEGITIMACIÓN PARA EL EJERCICIO DE LOS DERECHOS DE LOS TITULARES.

Los derechos de los Titulares podrán ejercerse por las siguientes personas:
- Por el Titular, quien deberá acreditar su identidad.
- 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 o para otro.

9. DEBERES DE PEGSA COMO RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES

Son deberes de PEGSA como responsable del tratamiento de datos personales los siguientes:
- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley 1581 de 2012;
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- Tramitar las consultas y reclamos formulados en los términos señalados en la Ley 1581 de 2012;
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
- Informar a solicitud del Titular sobre el uso dado a sus datos;
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

10. ENCARGADOS DE DATOS PERSONALES

Los datos personales entregados por parte de PEGSA. deben ser usados únicamente para el encargo encomendado, de conformidad con la autorización recibida y bajo los lineamientos establecidos por la misma.

En PEGSA. son encargados del tratamiento del dato personal, cualquier empleado que en desarrollo de sus funciones use, recolecte, almacene, circule o suprima datos personales. EL ENCARGADO se compromete con LA COMPAÑIA a verificar el estado de entrega de los datos personales, así como ofrecer las medidas de seguridad necesarias para velar por la seguridad del dato según las políticas propias de seguridad. EL ENCARGADO debe contar con todas las medidas técnicas y tecnológicas necesarias para velar por la seguridad del dato personal, así como prestar la mayor diligencia debida en la ejecución de su labor respecto de la protección y seguridad del dato personal, tanto en bases de datos digitales como físicas. Son también deberes del ENCARGADO del tratamiento del dato personal los siguientes:

- Responder por el uso, custodia y protección de los datos personales entregados. Responder hasta por la culpa levísima respecto de la protección y custodia de los datos personales entregados por PEGSA. Informar inmediatamente al oficial de Datos Personales de PEGSA. cualquier comunicación relativa a los datos personales, así como cualquier reclamo o consulta que reciba por parte del titular de los datos personales. Adoptar el conjunto de documentos que conforman el manual interno de políticas y procedimientos para salvaguardar la seguridad de los datos personales entregados.
- Garantizar que cuenta con adecuadas medidas de seguridad técnicas y físicas o digitales en el tratamiento de los datos personales, ya sean estas físicas o digitales.
- Realizar oportunamente la actualización, rectificación o supresión de los datos, tal como indican estas políticas.
- Actualizar la información reportada por el oficial de Datos Personales de PEGSA. dentro de los 5 días hábiles contados a partir de su recibo, ya sea actualización de datos, revocatoria de autorización, disposiciones relativas a reclamos o peticiones, etc.
- Garantizar que el tratamiento de los datos personales sea realizado según la finalidad establecida en la autorización.
- Cumplir en todo momento las instrucciones dadas por PEGSA.

- Salvaguardar en todo momento la intimidad, buen nombre, y demás derechos similares del titular del dato.
- Hacer firmar acuerdos de confidencialidad a los contratistas o trabajadores si en razón o con ocasión de las labores que presta directamente con PEGSA se tratan datos personales.
- Informar inmediatamente cualquier incidente o vulneración que se presente con los datos personales entregados por PEGSA.
- Cumplir con lo dispuesto en la presente política.
- No entregar los datos personales entregados por PEGSA. a ningún tercero, salvo que por disposición de PEGSA. se deba realizar dicha entrega.
- Entregar a PEGSA toda la información una vez termine la ejecución del contrato. Bajo ningún motivo EL ENCARGADO podrá guardar copia alguna de datos personales.
- Firmar el acta de entrega de los datos personales.

Cualquier conducta contraria a las establecidas en el conjunto de documentos que conforman las políticas y procedimientos de protección de datos personales o su omisión comprometerá la responsabilidad del encargado y será considerado como falta gravísima.

11. RESPONSABLES DE APLICACIÓN DE LA POLÍTICA

EL ENCARGADO es en todo caso y para todos los efectos es el responsable del cumplimiento del conjunto de documentos que conforman las políticas y procedimientos de datos personales, así como de las instrucciones dadas por PEGSA. para la ejecución del contrato. Cualquier conducta contraria a las establecidas en el conjunto de documentos que conforman las políticas y procedimientos de protección de datos personales o su omisión comprometerá la responsabilidad del encargado.

EL ENCARGADO responderá hasta por sus empleados y/o contratistas.

12. OFICIAL DE PROTECCIÓN DE DATOS Y RESPONSABLE DE LA ATENCIÓN A LOS TITULARES

PEGSA, como responsable del Tratamiento de Datos Personales, ha designado dentro de su estructura un Oficial de Protección de Datos Personales según disposición de la Guía para la Implementación del Principio de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio. El Oficial de Protección de Datos Personales, asume la función de proteger los Datos Personales dentro de la compañía, en cumplimiento de la normativa que rige la materia, así como del conjunto de documentos que conforman las políticas y procedimientos de protección de datos establecidas para tal fin dentro de la organización.

El Oficial de Protección de Datos de PEGSA será: El profesional de gestión documental o la persona que en su momento haga sus veces, quien se ubica en el domicilio de la sociedad en la Transversal 55 #98ª-66 ofc 411 Centro Comercial Iserra 100, teléfono: 6210345 y Correo electrónico: datos.personales@pegsa.com.co.

De conformidad con el procedimiento que más adelante se indica, cualquier petición, queja o reclamo relacionada con el manejo de datos personales, en aplicación de lo previsto en la Ley 1581 de 2012 y el Decreto 1377 de 2013, deberá enviarse a PEGSA, dependencia: Gestión Documental, Dirección: Transversal 55 #98ª-66 ofc 411 Centro Comercial Iserra 100, Teléfono: 6210345, Correo electrónico: datos.personales@pegsa.com.co.

13. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Y SU APOYO

El oficial de Seguridad de la información de PEGSA, será el oficial de Protección de Datos y su laborar será salvaguardar la información de la organización, procurando su buen uso bajo los fines autorizados y conservando su integridad y calidad. En el desarrollo de su labor actualizará, y pondrá en ejecución las políticas y procedimientos referentes a la seguridad de la información tanto física como electrónica y

establecidas en el conjunto de documentos que conforman las políticas y procedimientos de protección de datos personales.

Para el desarrollo de su función contará con el departamento de tecnología quien la asesora en temas técnicos, siendo el responsable de implementar los controles tecnológicos adecuados para salvaguardar la información de la organización.

14. PROCEDIMIENTOS

14.1. Procedimiento para la realización de consultas

Los titulares de datos personales o sus causahabientes, podrán solicitar la consulta de sus Datos Personales en los canales descritos en ésta políticas. Las consultas, deberán contener como mínimo lo siguiente:

- ✓ La identificación completa del titular,
- ✓ Los datos personales objeto de consulta,
- ✓ Dirección,
- ✓ Correo electrónico, y;
- ✓ En caso de ser causahabientes anexar el respectivo documento que lo demuestre.

- EL ENCARGADO que reciba una consulta por parte de un titular del dato personal deberá remitirla dentro de los dos (2) días siguientes al Oficial de Protección de datos personales. La solicitud deberá contener todos los datos adjuntados por parte del titular y el estado actual de la información que tiene el encargado sobre los datos personales del titular que consulta.

- La consulta será atendida por el oficial de protección de datos, en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la solicitud enviada ya sea mediante correo electrónico o del documento físico allegado.

- Cuando no fuere posible atender la consulta dentro de dicho término, el oficial de protección de datos Informará al interesado expresando los motivos de la demora y señalará la fecha en que se atenderá su solicitud en un tiempo máximo de cinco (5) días hábiles siguientes al vencimiento del primer término.

- Cuando la consulta no sea clara, no se entienda, o no cumpla los requisitos necesarios para desarrollar una respuesta por parte de oficial de protección de datos, ésta le informará al titular o al causahabiente para que nuevamente presente la consulta a más tardar dentro de los cinco (5) días hábiles siguientes al requerimiento por parte de la sociedad.

- Transcurrido dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, PEGSA. entenderá, que el Titular o causahabiente ha desistido de la consulta.

- En caso de que quien reciba la consulta 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.

14.2. Procedimiento para la realización de reclamos

Cuando el titular o causahabiente considere que la información contenida en nuestra Base de Datos deba ser objeto de corrección, autorización, supresión o revocación de autorización, podrá presentar reclamo a los canales de atención dispuesto para tal fin en estas políticas. Este reclamo deberá contener como mínimo lo siguiente:

- ✓ La identificación completa del Titular,
- ✓ Descripción de los hechos que dan lugar al reclamo,
- ✓ Dirección del domicilio,

- ✓ Correo electrónico, y;
- ✓ Acompañamiento de los documentos que el titular o causahabiente quiere hacer valer.

- EL ENCARGADO que reciba un reclamo deberá remitirla dentro de los dos (2) días siguientes al Oficial de Protección de datos personales. La solicitud deberá contener todos los datos adjuntados por parte del titular y el estado actual de la información que tiene el encargado sobre los datos personales del titular que consulta, así como el mecanismo de recolección de ese dato personal, ya sea porque fue entregado inicialmente por parte de PEGSA o recolectado por EL ENCARGADO. En este último caso EL ENCARGADO deberá adjuntar la autorización solicitada a este titular.

- Si el reclamo resulta incompleto PEGSA requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. Transcurrido dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, PEGSA. entenderá, que el titular o causahabiente han 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.

- 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.

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

14.3. Procedimiento para el trámite de la información que se encuentra en discusión

Cuando el titular o causahabiente considere que la información contenida en nuestra Base de Datos tenga información “en discusión”, es decir que no se encuentra de acuerdo con esa información, deberá presentar reclamo a los canales de atención dispuesto para tal fin en los canales descritos en las políticas. Este reclamo deberá contener como mínimo lo siguiente:

- ✓ La identificación completa del Titular,
- ✓ Descripción de los hechos u la información en discusión,
- ✓ Dirección del domicilio,
- ✓ Correo electrónico, y;
- ✓ Acompañamiento de los documentos que el titular o causahabiente quiere hacer valer.

- Una vez este recibido este tipo de reclamos se marcará la información y ésta información no podrá circular hasta que no se solucione la discusión.

- Si el reclamo resulta incompleto PEGSA requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. Transcurrido dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, PEGSA. entenderá, que el titular o causahabiente han desistido del reclamo.

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

14.4. Procedimiento para el trámite de la información que se encuentra en litigio judicial

Cuando una autoridad judicial, el titular o causahabiente informe a PEGSA. sobre información que se encuentre en litigio judicial se marcará la información y no se permitirá su circulación hasta que no se haya resuelto el litigio. Una vez PEGSA. sea informado de los resultados del litigio se realizarán las correcciones de acuerdo con la sentencia judicial correspondiente.

14.5. Procedimiento para el reporte de novedades a la SIC

Estos reportes procederán de la siguiente manera:

- **Reporte de PQR:**

  - ✓ Mensualmente se consolidará por base de datos la información de los reclamos que se tengan de acuerdo con la codificación de la Superintendencia de Industria y comercio.
  - ✓ Dicha información se subirá a la plataforma de la SIC.

- **Reporte de Incidentes de Seguridad:**

Una vez exista un incidente de seguridad se identificarán las bases de datos comprometidas.

- ✓ Se les comunicará a los titulares afectados
- ✓ Se subirá la información al sistema de la SIC por base de datos
- ✓ Se realizará la investigación pertinente y simultáneamente se procederá a recuperar la información expuesta, tomándose las medidas de control adecuadas.

14.6. Procedimiento para la gestión de usuarios

- **Procedimiento para crear un usuario nuevo:**

  - ✓ Para la creación de un nuevo usuario se creará desde recursos humanos quien dependiendo del perfil del cargo solicita a los dueños de la información los accesos requeridos en el formato GH-R-29.
  - ✓ Los dueños de la información aprueban los accesos.
  - ✓ El departamento de Tecnología crea los usuarios de acuerdo con lo autorizado.
  - ✓ Recursos Humanos le entrega el usuario al empleado, le hace firmar el compromiso de confidencialidad y le explica que deberá cambiar la clave cuando entre.
  - ✓ Recursos Humanos le envía copia de los accesos y del compromiso de confidencialidad al oficial de protección de datos con lo cual se informa al oficial de protección de datos del nuevo empleado y su usuario.

- **Procedimiento para modificaciones de usuarios:**

Para la modificación de usuarios se gesta desde recursos humanos quien dependiendo del perfil del cargo solicita a los dueños de la información los accesos requeridos e indica los accesos que se deben eliminar en el formato GH-R-29.

- ✓ Los dueños de la información aprueban los accesos.
- ✓ El departamento de Tecnología modifica el usuario de acuerdo con lo autorizado.
- ✓ Recursos Humanos le entrega el usuario al empleado, le hace firmar los cambios.
- ✓ Recursos Humanos le envía copia de los accesos y del compromiso de confidencialidad al oficial de protección de datos con lo cual se informa al oficial de protección de datos de los cambios del empleado y su usuario.

- **Procedimiento para eliminación de un usuario:**

  Para la eliminación de usuarios se tendrá en cuenta si por motivos de trazabilidad o logs se puede o no borrar el usuario, si no se puede borrar se dejaran deshabilitados en el Active Directory.

bloqueo definitivo. Para la eliminación de la cuenta de correo se gesta desde recursos humanos quien informa a Tecnología y al oficial de protección de datos que el empleado se retira y quien asumirá sus funciones.

- ✓ El departamento de tecnología enruta el correo al nuevo responsable de las funciones
- ✓ El departamento de tecnología realiza un backup del correo del usuario y se guarda la información
- ✓ EL nuevo responsable tendrá acceso al correo anterior por un mes y posteriormente en caso de necesitar tendrá acceso al backup del correo.

- **Procedimiento para Bloqueo de usuarios**

  - **Bloqueo Temporal**

  El bloqueo temporal sea da cuando el usuario ha sido sancionado. Para lo cual Recursos Humanos informa a Tecnología mediante correo electrónico e inmediatamente se hace el bloqueo del usuario por el tiempo que vaya a estar ausente.
  - ✓ El usuario solicitará por escrito el desbloqueo una vez se reincorpore.
  - ✓ Bloqueo Definitivo
  - ✓ El bloqueo definitivo se da cuando el empleado se retira de la organización. Para lo cual Recursos Humanos informa a Tecnología mediante correo electrónico e inmediatamente se hace el bloqueo del usuario.
  - ✓ Los usuarios no se eliminarán para no perder el rastro en los logs de auditoria.

  - **Bloqueo Definitivo**

    - ✓ El bloqueo definitivo se da cuando el empleado se retira de la organización. Para lo cual Recursos Humanos informa a Tecnología mediante correo electrónico e inmediatamente se hace el bloqueo del usuario. Lo cual solo aplica para los sistemas que tengan logs y para los cuales el rastreo se vea afectado por el borrado del usuario.

14.7. Procedimiento para la asignación de responsabilidades y autorizaciones en el tratamiento de la información personal

- **Procedimiento para un empleado nuevo:**

Cada vez que ingrese un empleado nuevo, recursos humanos informará al oficial de protección de datos las funciones que este empleado cumplirá y de acuerdo con el perfil del cargo y con la autorización de los dueños de la información se le otorgarán mediante comunicación formal las autorizaciones para el tratamiento de ciertos datos personales y se le explicarán sus responsabilidades.

- ✓ El oficial de protección de datos personales le hará entrega personal de la comunicación al empleado nuevo y le hará la capacitación en el sistema de gestión de protección de datos personales, la cual se realizará dentro del programa de inducción y re inducción que tiene la organización.
- ✓ El recibido de la comunicación debe constar en el archivo de oficial de protección de datos.

- **Procedimiento para un empleado trasladado:**

Cada vez que un empleado cambie de funciones, recursos humanos le informará al oficial de protección de datos las funciones que este empleado cumplirá y de acuerdo con el perfil del cargo y con la autorización de los dueños de la información se le modificarán las autorizaciones, las cuales se le informarán mediante

comunicación formal. El recibido de la comunicación debe constar en el archivo de oficial de protección de datos.

- **Procedimiento para la revocatoria en el tratamiento de datos personales:**

  - **Revocatoria por retiro**

    - ✓ Recursos humanos informará al oficial de protección de datos que el empleado se retira de la compañía y el oficial de protección de datos procederá a remover las autorizaciones y asegurarse que el empleado no tenga acceso a los datos personales que maneja la organización.
    - ✓ El oficial de Protección de las autorizaciones personales le notificará por escrito al empleado la revocatoria para el tratamiento de los datos de personales y le explicará que de ese momento en adelante no podrá realizar ningún tratamiento.

  - **Revocatoria por sanción**

    - ✓ En el momento en que se identifique una posible falta en el manejo de la información personal de la compañía, el oficial de protección de datos le informa a Recursos Humanos para que realice el proceso disciplinario conforme a la ley laboral y al reglamento interno de trabajo.
    - ✓ Recursos humanos informará al oficial de protección de datos los resultados de la investigación disciplinaria y en caso de ser sancionado el oficial de protección de datos personales procederá a revocar la autorización para el tratamiento de los datos personales.
    - ✓ El oficial de Protección de datos personales le notificará por escrito al empleado la revocatoria para el tratamiento de los datos de personales y le explicará que de ese momento en adelante no podrá realizar ningún tratamiento.
    - ✓ El recibido de la comunicación debe constar en el archivo de oficial de protección de datos.

14.8. Procedimiento para la creación y validación de datos personales

En el momento que sea necesario crear un nuevo registro de datos personales se debe solicitar al titular la siguiente información:

- ✓ Autorización para la recolección y tratamiento de los datos personales de acuerdo con su vinculación a la organización.
- ✓ Formato de registro con la información necesaria, el cual contará con las validaciones adecuadas para verificar tamaños de los campos, tipos de valores y composición.
- ✓ Rut e información financiera en caso de requerirse para el sistema contable.
- ✓ Con la información solicitada el oficial de protección de datos procederá a coordinar la creación del registro en el correo electrónico corporativo y en caso de ser necesario en el sistema contable.

14.9. Procedimiento para la auditoria de los sistemas de información y del sistema de datos personales

- **Procedimiento para la realización de monitoreos:**

  - ✓ Cada trimestre el oficial de protección de datos personales o un tercero contratado para el efecto, tomará una muestra aleatoria de las bases de datos personales y buscará las autorizaciones; igualmente verificará los logs de auditoria cotejando las autorizaciones y accesos permitidos a las personas que tuvieron acceso a esa información. Adicionalmente tomará una muestra de autorizaciones y permisos de usuarios y verificará los accesos y uso de las autorizaciones.
  - ✓ El informe que se emita será discutido con el oficial de protección de datos personales, los dueños de la información y el área de tecnología.
  - ✓ Una vez discutido el informe se debe realizar un plan de trabajo cuya verificación será parte del alcance del siguiente monitoreo.

- **Procedimiento para la realización de auditorias**

Cada año un auditor capacitado realizará la auditoria de todo el sistema de protección de datos personales y de los controles de los sistemas de información, enfatizando en las áreas de:

- ✓ Seguridad de la información
- ✓ Respaldos y Continuidad de negocio
- ✓ Operaciones de los sistemas de información
- ✓ Control de cambios y desarrollos de nuevos sistemas

La auditoría se realizará siguiendo las mejores prácticas de auditoria emitidas por el instituto de auditores internos y por la asociación de auditores de sistemas de información y control.

El informe que se emita será discutido con el oficial de protección de datos personales, los dueños de la información y el área de tecnología. Una vez discutido el informe se debe realizar un plan de trabajo cuya verificación será parte del alcance del siguiente monitoreo y de la siguiente auditoria.

15. Referencias

- Ley 1581 de 2012
- Decreto 1074 de 2013
- Decreto 886 de 2014

16. CONTROL DE CAMBIOS

Fecha	Descripción	Versión
01/02/2017	Creación del documento	00