	MANUAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES	**VERSIÓN: 004**

ELABORADO POR:	**REVISADO POR:**	**APROBADO POR:**
JyJ Nombre	Adriana Buitrago Nombre	Mauricio Ángel Nombre
Profesional TI Cargo	Líder Proyecto Cargo	Director Sistemas de Información Cargo
Firma	Firma	Firma
Fecha: 12-11-2019	Fecha: 12-11-2019	Fecha: 12-11-2019

1. CONTROL DE CAMBIOS

FECHA DE APROBACION	VERSIÓN	CONTROL DE CAMBIOS
12-11-2019	00	Creación del documento.
25-03-2021	01	Modificación párrafo numeral 6.1 y Adición 6.3 Gestión.
02-12-2021	02	Modificación y adición de Gestión, control y aprobación de documentos.
02-04-2022	03	Modificación y ajuste control interno de solicitudes.
02-12-2025	04	Modificaciones generales

2. OBJETIVOS

- Cumplir en los tiempos establecidos por la Ley las solicitudes de titulares, en materia de protección de datos personales.
- Establecer una política específica para el acceso o tratamiento de información personal de las bases de datos con información personal sensible, así como la asignación de responsabilidades y autorizaciones en el tratamiento de la información personal.
- Enunciar los parámetros generales establecidos para que el encargado de tratamiento de información interna de la compañía realice la correcta administración de la plataforma de la SIC.
- Proporcionar los parámetros establecidos al interior de FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO para atender y dar respuesta, gestionar y tramitar los Incidentes de seguridad en el Área de sistemas de Información para todos los servicios de Infraestructura TI y en especial aplicaciones críticas y bases de datos que tienen incidencia para la Ley de protección de datos.

3. ALCANCE

La actual política es establecida para los procedimientos de Recolección de información del proceso interno con terceros de la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO y Bases de datos internas dispuestas de forma física y aquellas que se encuentran en los diferentes aplicativos de empleados para el desarrollo de sus objetivos institucionales; la administración de incidentes aplica a los servicios definidos y suministrados, dando cumplimiento al Régimen de Protección de Datos Personales Ley 1581 de 2012 y Decreto 1377 de 2013.

4. DEFINICIONES

Para efectos del presente manual y en concordancia con la normatividad vigente en materia de protección de datos personales, se establecen las siguientes definiciones:

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
Activo: Componente del proceso de negocios. Los activos pueden incluir, gente, edificios, sistemas computacionales, redes, registros papel, faxes, etc.
Acuerdo de Niveles de Servicio (Service Level Agreement - SLA): Acuerdo escrito entre el proveedor de servicios y el cliente sobre los niveles de servicio acordados entre ambas partes.
Administración de Niveles de Servicio (Service Level Management - SLM): El proceso de definir, acordar, documentar y manejar los niveles de servicio del cliente de TI, que son requeridos y justificados en costo.
Ambiente: Colección de hardware, software, redes de comunicación y procedimientos que trabajan de forma conjunta para proveer un cierto tipo de servicios computacionales. Puede haber uno o más tipos de ambientes en plataformas físicas, por ejemplo, pruebas, producción o desarrollo.
Análisis de Impacto: La identificación de los procesos críticos de negocio, daño potencial y pérdida que pueden causarle al negocio, resultantes de una interrupción en las operaciones de los procesos. El análisis de impacto al negocio identifica:

- La forma de tomar la pérdida o daño.
- Qué probabilidad de escalar se tiene, dentro del tiempo que le sigue al incidente.
- Staff mínimo, facilidades y servicios necesarios para permitirle a los procesos de negocio continuar con su operación mínima aceptable.
- El tiempo dentro del cual los servicios deben ser recuperados. El tiempo dentro del cual la recuperación total del negocio es alcanzada, si es identificada.

Análisis de Riesgo: Identificar y evaluar el nivel de riesgo, tomando en cuenta los activos expuestos o amenazados.
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.
Calendario de Cambios Programados (Forward Scheduled Changes - FCS): Calendario que muestra a detalle todos los cambios aprobados para su implementación con sus respectivas fechas para ello. Deberá realizarse un acuerdo entre el cliente y el negocio, Administración de los Niveles de Servicio, Mesa de Servicio o Mesa de Ayuda y Manejo o Administración de la Disponibilidad. Una vez realizado el acuerdo, la mesa de servicio deberá comunicar

a la comunidad usuaria cuando no se podrá disponer de los servicios que estén relacionados con los cambios planeados, a través de los medios más efectivos dentro de la organización.

Calidad del Servicio: Nivel de servicio contratado o acordado entre el proveedor de servicios y el cliente.

Cambio: Modificación adicional aprobada sobre la línea base de: hardware, red, software, aplicación, ambiente, sistema, o documentación asociada.

Cambios normales: Son aquellas solicitudes de cambio que son requeridas por las unidades de negocio o internamente por la organización de TI para mejorar un servicio. Este tipo de cambios se clasifican también como cambios planeados, ya que se tramitan en el proceso de administración de cambios con todos sus pasos, entre otros el de análisis y evaluación de riesgos, impacto y recursos necesarios para realizar el cambio; puede incluso participar el Consejo de Control de Cambios (Change Advisory Board - CAB).

Cambios urgentes: Son solicitudes de cambio, que por su naturaleza pueden provenir de un incidente con un alto impacto o de un problema que afecte gravemente los niveles de servicio comprometido, y cuya única solución sea a través de un cambio.

Cierre: Cuando un cliente interno o externo a la compañía está satisfecho por la resolución del incidente que levantó.

Cliente: Receptor de un servicio, normalmente servicio al cliente es responsable del costo del servicio, ya sea de manera directa a través de la transferencia de costos o indirectamente en términos de las necesidades del negocio.

Control de Cambio: Procedimiento para asegurar que todos los cambios están controlados, incluyendo el análisis, toma de decisiones, sujeción, aprobación, implementación y post-implementación del cambio.

Control de Proceso: Proceso de planeación y regulación con el objetivo de ejecutar el proceso de una manera efectiva y eficiente.

Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular de la información, como por ejemplo la historia clínica.

Dato Público: Es el dato que la ley o la Constitución Política determina como tal, como por ejemplo el número de cedula del representante legal de una sociedad, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva legal y los relativos al estado civil de las personas.

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

Dato 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 promuevan intereses de cualquier partido político, la salud, la vida sexual y los datos biométricos.

Datos Personales: Toda aquella información asociada a una persona natural determinada o determinable que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Adicionalmente, existe información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

Disponibilidad: Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo. Usualmente es expresado por una relación de disponibilidad, por ejemplo: La proporción de tiempo que el servicio está disponible para uso del servicio por el usuario, dentro del horario de servicio acordado.

Documentación del Cambio: Requerimiento de Cambio (RFC), forma de control, orden y registro del cambio.

Elementos de Configuración (Configuration Item - CI): Componente de la infraestructura o elemento, tal como el requerimiento de cambio asociado a la infraestructura que es o estará bajo control de la Administración de la Configuración. Un CI pueden variar mucho en complejidad, tamaño y tipo, desde un sistema completo incluyendo todo el hardware, software y documentación, hasta un solo módulo o un pequeño componente de hardware.

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.

Factores Críticos de Éxito (FCE): Un medidor del éxito o madurez de un proyecto o proceso. Puede ser un estado, entregable o meta. Un ejemplo podría ser: “La elaboración de toda la estrategia de tecnología”

Incidente de seguridad: Un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la violación de una medida de seguridad establecida por la compañía. Como ejemplos de incidentes de seguridad podemos enumerar:

- Acceso no autorizado
- Robo de contraseñas
- Robo de información
- Denegación de servicio

Incidente: Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio.

Infraestructura de TI: La suma de los activos de la organización de TI como; hardware, software, facilidades de telecomunicación de datos, procedimientos y documentación.

Interfaz: Interacción física o funcional en los límites entre elementos de la configuración.

ISO 9001: Conjunto de estándares internacionales aceptados, referentes a los sistemas de administración de la calidad.

ITIL: La librería de Infraestructura de TI de la Oficina Gubernamental de Comercio de Inglaterra (OGC ITIL), Es un conjunto de guías para la administración y provisión de los servicios operativos de TI.

Mesa de ayuda: Punto único de contacto dentro de la organización de TI, para los usuarios.

Métrica: Elemento medible de un proceso o una función.

Nivel de Servicio: Expresión de un aspecto del servicio, en términos cuantificables y definitivos.

Operaciones: Todas las actividades y medidas para habilitar y/o mantener el uso de la infraestructura de TI.

Prioridad: Secuencia con la que un problema o incidente tiene que ser resuelto, basado en impacto y urgencia.

Problema: Causa principal desconocida de uno o varios incidentes.
Proceso de Negocios: Grupo de actividades de negocio comprometidas por una organización, persiguiendo un fin u objetivo común Los típicos procesos de negocios incluyen recepción de órdenes, servicios de mercadotecnia., venta de productos, servicios de entrega, distribución de productos, facturación por servicios, contabilización por dinero recibido. Un proceso de negocio normalmente depende del soporte de varias funciones de negocio.
Proceso: Serie de acciones, actividades, cambios, etc. conectadas. Realizadas por agentes que tienen el propósito de satisfacer o lograr un objetivo.
Proveedor: Organización encargada de proveer los servicios de TI.
RNBD: Registro Nacional de Bases de Datos.
Recursos: Ayudan a proveer los requerimientos de los clientes de TI. Los recursos son usualmente computadoras y equipo relacionado, software, facilidades (edificio, sites, etc.) y gente.
Requerimiento de Servicios: Cada servicio que no sea una falla provista por la infraestructura de TI.
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.
Servicio de TI: Conjunto de facilidades de TI y de no TI, proveídos por el servidor de dichos servicios, que satisface con una o varias necesidades de los clientes y que el cliente lo percibe como un todo.
SIC: Superintendencia de Industria y Comercio
Sistema: Compuesto integral que consiste en uno o más procesos, hardware, software, facilidades y gente, que tiene la capacidad de satisfacer una necesidad u objetivo.
Solución o Soporte Remoto: Incidente o problema solucionado sin la necesidad de presencia física de un elemento del staff de soporte. Nota: Esta modalidad minimiza el tiempo de falla, por lo que ayuda a minimizar el costo efectivo de falla.
TI: Tecnología de Información.
Tiempo de Caída: Periodo de tiempo que un servicio o dispositivo está fuera de servicio, dentro de los tiempos de servicio acordados.
Titular: Persona natural cuyos datos personales sean objeto de tratamiento, y quien otorga autorización para el tratamiento de los mismos.
Transferencia de datos a terceros países: 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 los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un tratamiento efectuado por el encargado, por cuenta del responsable.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5. GESTIÓN DE SOLICITUDES DE TITULARES

Para la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso por el respeto de los datos de personas naturales, en su tratamiento y finalidades, por lo anterior como responsable y/o encargados del tratamiento establecemos mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares, con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos.

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO previamente ha definido que el canal establecido para atender solicitudes de titulares son los siguientes:

FEDEPANELA	FONDO DE FOMENTO	CANAL
	X	ffpprotecciondedatos@fedepanela.org.co
X		fedeprotecciondedatos@fedepanela.org.co

y físicamente en la dirección **Carrera 49 B No 91-48 La Castellana.**

El departamento encargado por parte de FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO responsable inscrito ante la SIC de recibir, consolidar, verificar el carácter legal de la solicitud es el área de sistemas de información.

El Titular podrá consultar de forma gratuita sus datos personales:

i. al menos una vez cada mes calendario, y
ii. 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, el responsable solo podrá cobrar al titular los 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 (SIC), cuando esta así lo requiera, el soporte de dichos gastos.

5.1. Verificación de identidad del titular

El Área de sistemas de información debe conocer que las solicitudes pueden ser realizadas por las siguientes personas y es necesario validar su identidad.

a) A los Titulares, sus causahabientes o sus representantes legales;
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
c) A los terceros autorizados por el Titular o por la Ley.

5.2. Tiempo establecido para la respuesta al titular

La consulta se formulará por el medio habilitado por el responsable o encargado del tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de **diez (10) días hábiles** contados a partir de la fecha de recibo de esta. 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.

5.3. Establecimiento del 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 esta Ley, podrán presentar un reclamo haciendo uso del canal establecido y bajo los siguientes criterios:

a) El reclamo debe contener
   - Nombres y apellidos del titular.
   - Número de identificación del titular.
   - Datos de localización del titular.
   - Descripción de los hechos que dan lugar a la consulta o reclamo.
   - Documentos que considere soportan su consulta o reclamo.
   - Medio por el cual desea recibir respuesta.
   - Nombre del peticionario, el cual, si es diferente al titular, debe adjuntar los documentos que le permitan actuar en su nombre.

b) El término máximo para atender el reclamo será de **diez (10) 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 **cinco (5) días hábiles** siguientes al vencimiento del primer término.

5.4. Reclamos incompletos.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los **cinco (5) días hábiles** 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.

5.5. Distribución interna de la solicitud

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA Y FONDO DE FOMENTO PANELERO tienen varios responsables internos del tratamiento y recolección de datos personales, es deber del área de sistemas de información una vez verificados los requisitos antes establecidos de la solicitud del titular, distribuir al interior a cada responsable los datos del titular, para identificar las bases de datos en las cuales se tiene registro a su nombre.

Cada responsable deberá responder de manera oportuna en un máximo de **48 horas**, confirmando si los datos del titular se encuentran o no en su base de datos.

Una vez identificados los datos del titular, se consolidan y se le da respuesta al titular según su requerimiento

5.6. Derechos del Titular

- Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento.
- Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- 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 SIC 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.

Una vez contemplada la solicitud expresa del titular es deber del área de Sistemas de información, dar las instrucciones a los responsables internos de las bases de datos, en base a las disposiciones establecidas en respuesta a la solicitud del titular, y divulgar a todos los responsables las acciones tomadas a través de un mecanismo eficiente de comunicación, posteriormente debe validar que se haya cumplido efectivamente, la actualización, supresión, o simplemente que se encuentre la información en un estado de permisos revocados para que este titular sea identificado internamente, y tener especial cuidado del tratamiento que se realice de sus datos.

5.7. Contestación al titular y evidencia

Es deber del área de Sistemas de información dar la contestación al titular dentro de los plazos establecidos y dejar evidencia de dicha contestación, de manera que sea veraz e inequívoca.
Si es a través de mecanismos electrónicos es importante mantener copias de los correos y en lo posible mantenerlos en mecanismos que no permitan su posterior modificación como CDS o DVD, de manera que mantengan sus fechas originales de creación y modificación.

5.8. Bases de datos como encargados o incompetencia para resolverlo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de cinco (5) días hábiles e informará de la situación al interesado.

Si la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO no son las entidades competentes para resolver un reclamo, darán traslado de este a quien corresponda en un término máximo de **CINCO (5) días hábiles,** si el nuevo responsable es identificable se informará de la situación al interesado para que pueda hacer seguimiento o identifique claramente la entidad a la cual debe dirigirse.

Para casos de bases de datos suministradas, en donde la **FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO** obra en nombre de otra entidad u organización (responsable), esta es considerada como encargada del tratamiento de los datos, por lo tanto debe:

a) Reportar al responsable dentro de los **cinco (5) días hábiles** siguientes, la solicitud del titular.
b) Mantenerlo informado del proceso de atención y la respuesta de las solicitudes.
c) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente política y en los tiempos que establezca la Ley.
f) Abstenerse de circular información que esté siendo controvertida por el usuario y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
g) Permitir el acceso a la información únicamente a las personas autorizadas por el usuario o facultadas por la Ley para dicho efecto.
h) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los usuarios.
i) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

5.9. Contestaciones a la Superintendencia de Industria y Comercio.

Es deber del área de Sistemas de información dar las respuestas y pruebas necesarias a la Superintendencia de Industria y Comercio ante cualquier investigación realizada, demostrando la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable pues serán tenidas en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la Ley y normativa concordante, proporcionando la siguiente información, así como cualquiera que requiera este organismo.

Dentro de la información que se debe suministrar a la SIC se encuentra:

- La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
- La naturaleza de los datos personales objeto del tratamiento.
- El tipo de Tratamiento.
- Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
- En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada, y una explicación sobre la relevancia de los datos personales en cada caso.
- En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.

6. TRATAMIENTO INTERNO DE DATOS PERSONALES

6.1. Disposiciones Generales

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO tienen varios encargados al interior o responsables internos del tratamiento y recolección de datos personales, y el área de Sistemas de información se establece como encargado de atención de solicitudes de titulares.

Es responsabilidad del área de sistemas de información la distribución de la solicitud mediante los siguientes correos:

FEDEPANELA	FONDO DE FOMENTO	CANAL
	X	ffpprotecciondedatos@fedepanela.org.co
X		fedeprotecciondedatos@fedepanela.org.co

a cada uno de los responsables del tratamiento de los datos que tengan bajo su custodia o control la base de datos donde se encuentre el dato a tratar, el seguimiento y supervisión de la atención en los tiempos establecidos para la misma, así como de desarrollar las tareas de revisión y control que garanticen de forma técnica que las actividades realizadas por cada uno de los responsables fueron las adecuadas para dar cumplimiento a la solicitud.

Algunas bases de datos registradas que maneja FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO están sujetas a la generación de análisis con el fin de realizar operaciones estadísticas, generar reportes, informes con datos generalizados mas no puntuales, que con la difusión puedan llegar a afectar la privacidad de los titulares.

Cada responsable debe al interior de la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO responder por la recolección y tratamiento de los datos que se encuentran en la base de datos en su custodia o control, y tener específico control sobre aquellos casos en donde el titular no ha dado su aprobación para el tratamiento de los datos.

El área de Sistemas de información es responsable de construir y ejecutar **auditorias de control** y mejoramiento bajo los planes y cronogramas del área, de tal forma que garantice el cumplimiento de los lineamientos indicados en este Manual.

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

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

a) 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.

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

Se prohíbe expresamente la recolección o tratamiento de manera individual de datos personales, toda base de datos debe ser unificada en un solo repositorio de información definido por el área y controlado a través de permisos de usuario.

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO deben construir y ejecutar auditorias periódicas que permitan controlar y realizar seguimiento a los diferentes lineamientos de seguridad para las bases de datos, así como al cumplimiento por parte del proceso operativo y administrativo de todas las normas que tengan lugar para el fin de protección de datos.

El área de sistemas de información debe consolidar y unificar la política de seguridad de tal forma que se puedan tener lineamientos claros con su respectiva divulgación y de esta manera una efectiva aplicación o ejecución por parte de los responsables, adicionalmente esta área es la responsable de controlar desde la perspectiva tecnológica las actividades que se desarrollan en este procedimiento.

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO debe desarrollar campañas y programas de sensibilización con los colaboradores, contratistas y beneficiarios de los programas y proyectos, sobre sus derechos en relación con sus datos personales y su uso adecuado, especialmente en relación con las tecnologías de información.

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO tiene distribuido su archivo físico entre sus áreas y diferentes coordinadores de región, lo que le permite asegurar, organizar y custodiar de forma adecuada su registro de archivo físico dando la responsabilidad de esta a cada uno de sus encargados.

La FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO debe garantizar que todas las áreas, realicen la recolección y formalización de los diferentes formatos de autorización para el tratamiento de los datos en los momentos definidos para tal fin. De igual manera debe garantizar sin perjuicio de las excepciones previstas en la Ley, la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Se han dispuesto diferentes mecanismos físicos y tecnológicos por parte de la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO, para mantener las evidencias de autorizaciones otorgadas por los titulares.

6.2. Tratamiento De Las Bases De Datos

Para el tratamiento de las bases de datos, la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO ha dispuesto del documento de administración de bases de datos, donde se encuentra la información detallada de las bases que se encuentran actualmente registradas y bajo responsabilidad de la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO.

6.3. Gestión, control y aprobación de documentos

1. Solicitud de Atención (Terceros)

En el caso de solicitudes de entidades que requieran contratos de transmisión de datos personales, la entidad debe enviar una comunicación o un oficio formal solicitando el proceso y debe ir acompañado del diligenciamiento del siguiente formulario: https://docs.google.com/forms/d/e/1FAIpQLSdjIhKFrt_dxqzy0iMhoHagYniLhALMBpb52510f8IbsqSSQg/viewform?usp=sf_link.
La atención no superará los cinco (5) días hábiles después de enviado el requerimiento.

Las entidades a las cuales se les debe priorizar la atención son:

1. Fiscalía General de la Nación.
2. Algún ente judicial que actúe en nombre de la Ley (jueces de la república, investigadores judiciales entre otros).
3. Contraloría.

4. Procuraduría.
5. Superintendencia de Industria y Comercio.
6. Ministerio de Agricultura y Desarrollo Rural.

2. Solicitud de Atención (Contratistas)

Todas las solicitudes, requerimientos y preguntas de tratamiento de datos personales deben ser remitidas al correo gestionspdp@fedepanela.org.co, la atención no superará los **cuatro (4) días hábiles** después de enviado el requerimiento.

3. Gestión y procesos de formularios (Contratistas)

En el caso de las bases de datos que requieran recolección digital, es decir vía formularios web, estos deben estar asociados al correo autorizado en el manual interno de seguridad de la información, el cual es: gestionspdp@gmail.com. Además, deben contar con el párrafo de tratamiento de datos y revisión de este por parte del sistema de protección de datos personales, para dicho proceso se debe enviar un correo de solicitud de la creación del formulario web especificando el formato borrador ya creado por el interesado con la información que se requiere solicitar, para la fácil migración. El formato ya ajustado no superará los **cuatro (4) días hábiles** en entregarse al área solicitante después de recibir el correo del interesado. Una vez creado el nuevo formulario en el drive y organizarlo en la carpeta de su área; el sistema de protección de datos personales compartirá la información recolectada y el formulario proyectado a las personas indicadas en la solicitud inicial. Adicionalmente estos permisos caducaran a final de cada vigencia anual.

4. Respuesta a solicitud

La respuesta se dará por parte del sistema de protección de datos personales mediante el canal: fedeprotecciondedatos@fedepanela.org.co; ffpprotecciondedatos@fedepanela.org.co o gestionspdp@fedepanela.org.co según sea el caso.

6.4. Manejo de imágenes y videos

En cuanto al manejo y uso de imágenes y videos, se establecen los siguientes lineamientos:

1. En el caso de requerir autorización de una persona para su uso de imagen en campañas publicitarias, se debe solicitar el diligenciamiento del formato de autorización de tratamiento de datos personales, formato que previamente ha sido proyectado y evaluado entre el sistema y el área que recolecta la información.

2. En el ejercicio de alguna actividad de carácter privado, si se usan dispositivos de grabación o toma de fotografías en el transcurso de este, se debe poner el anuncio o aviso de tratamiento de datos personales en la presentación, stand u otro lugar visible, el párrafo es el siguiente:

   "De conformidad con lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013 FEDEPANELA y FONDO DE FOMENTO PANELERO informa que todos los datos o imágenes captados y utilizados dentro de este evento, serán tratados conforme a la política de protección de datos de Fedepanela y Fondo de Fomento Panelero, y según las finalidades allí expuestas. las cuales podrán ser consultadas en www.fedepanela.org.co y www.sipa.org.co"

3. Se debe tener en cuenta que los listados de asistencia, ya sean virtuales o físicos, deben contar con la autorización para la captación de imágenes y videos en las reuniones que se realicen, así como la de tratamiento de datos personales. El área encargada de recolectar dicha información deberá solicitar la proyección de dichas autorizaciones al sistema de protección de datos personales de acuerdo con la finalidad que se requiera.

4. Para el caso de las autorizaciones **físicas** en las que haya recolección de imágenes y videos se debe enviar los originales a la oficina central en una carpeta marcada de la siguiente manera:

Autorizaciones Tratamiento de datos personales
•Departamento •Municipio •Nombre del evento •Convenio •Encargado en campo •Nombre del coordinador •Año

**En el caso de los convenios que requieran las autorizaciones originales, se debe enviar a la oficina central la digitalización del original al correo electrónico del director del área en la que se ejecutó el convenio, con copia a gestionspdp@fedepanela.org.co

5. En la oficina central se establecerá el anuncio de grabación de CCTV.

6. En cuanto a las solicitudes de revisión de las grabaciones en la plataforma zoom de las reuniones que se llevan a cabo en el ejercicio de las actividades de Fedepanela y Fondo de Fomento Panelero, ya sea las guardadas en la nube o en los usuarios administradores, estas no se deben enviar a correos, se puede permitir ver o consultarlas mediante la red corporativa u otro canal autorizado, previa autorización entregada por responsable de salvaguardar la información.

6.5. Seguimiento del sistema de protección de datos personales en las áreas.

En este manual se establecen los lineamientos o principios generales del sistema de protección de datos personales, la aplicabilidad de estos es responsabilidad de cada una de las áreas del Fondo de Fomento Panelero, sin embargo, el sistema de protección de datos personales podrá realizar validaciones de forma autónoma y aleatoria con el fin de verificar que se implementen, ejecuten y cumplan.

7. ADMINISTRACIÓN PLATAFORMA SIC

7.1 Actualizaciones de la SIC

La información contenida en el RNBD deberá actualizarse, como se indica a continuación:

1. Dentro de los primeros **diez (10) días hábiles** de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada.
2. Son cambios sustanciales los que se relacionen con la finalidad de la base de datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información y la transferencia y transmisión internacional de datos personales
3. Dentro de los **quince (15) primeros días hábiles** de los meses de febrero y agosto de cada año, a partir de su inscripción, los responsables del tratamiento deben actualizar la información de los reclamos presentados por los Titulares.
4. Como mínimo anualmente, entre el 2 de enero y el 31 de marzo, a partir de 2018.

7.2 Reportes en la SIC.

Incidentes de seguridad. Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, que deberán reportarse al RNBD dentro de los **quince (15) días hábiles** siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
Reclamos presentados por los Titulares. Corresponde a la información de los reclamos presentados por los Titulares ante el responsable y/o el Encargado del Tratamiento, según sea el caso, dentro de un semestre calendario (enero-junio y julio-diciembre). Esta información se reportará teniendo en cuenta lo manifestado por los Titulares y los tipos de reclamos prestablecidos en el registro. El reporte deberá ser el resultado de consolidar los reclamos presentados por los Titulares ante el responsable y el (los) Encargado (s) del Tratamiento.

8 GESTION DE INCIDENTES DE SEGURIDAD

8.1 Recepción del reporte del incidente

Cualquier usuario, funcionario interno o externo debe reportar lo que considere un incidente de seguridad al área de Sistemas de Información o al encargado de seguridad de la FEDERACIÓN NACIONAL DE PRODUCTORES DE PANELA y FONDO DE FOMENTO PANELERO, de manera inmediata se realiza su verificación, clasificación y se procederá a su registro.

8.2 Clasificación del incidente de seguridad

Es responsabilidad del área de sistemas de información realizar una clasificación previa del incidente en función de:
Potencial impacto del incidente: de acuerdo con la afectación de los servicios:

- Alta
- Media
- Baja

Tipo:

- Acceso no autorizado a sistemas
- Denegación de servicio
- Divulgación de información sensible
- Infección de Malware.
- Rasomware (virus).
- Severidad.

8.3 Identificación de procesos afectados

Es responsabilidad del área de sistemas de información realizar una evaluación lo más rápido posible y de manera efectiva de las aplicaciones y procesos afectados, tanto en la red interna como en los servicios publicados.

8.4 Notificación a jefes de área y responsables

Una vez evaluado el impacto que generará el incidente, se debe reportar inmediatamente al área de sistemas de información, quien a su vez realizará junto con el encargado de seguridad, la notificación a las áreas afectadas y realizará el plan de respuesta, las medidas de contención y mitigación de impacto.

8.5 Solicitud de avales

En el caso de que el sistema afecte aplicaciones críticas, el área de sistemas de información debe reunirse con los jefes de los servicios encargados o con el director general para solicitar su aval en los procesos a ejecutar.

8.6 Ejecución de medidas

En cabeza del proceso del área de sistemas de información y en ejecución de los funcionarios asistentes o encargados externos de cada proceso, se proceden a realizar las actividades de mitigación y medidas preventivas y correctivas de la siguiente manera:

8.6.1 Definir hora adecuada de pruebas en horas de bajo tráfico
8.6.2 Tomar algunas medidas de contingencia:
- 8.6.2.1 Definir estrategias de contingencia para activos críticos
- 8.6.2.2 Realizar respaldos de la información de los activos involucrados
- 8.6.2.3 Guardar en formato electrónico y físico configuraciones de equipos involucrados
- 8.6.2.4 Realizar monitoreo de los servicios durante las pruebas
- 8.6.2.5 Se debe monitorear el tráfico de la red:
  - 8.6.2.5.1 Utilización de los segmentos críticos
  - 8.6.2.5.2 Utilización de CPU en servidores críticos

8.7 Registro de medidas y solución

El área de sistemas de información, procederá a realizar los registros y documentación tanto del incidente, como de las medidas tomadas y los resultados. En caso de que existan medidas transitorias, también deben ser documentadas.

8.8 Análisis de consecuencias

Una vez ejecutado el plan de mitigación, se debe realizar un análisis de las consecuencias y del resultado del incidente, estableciendo si se generó:

- Robo de información
- Afectación de bases de datos
- Afectación de bases de datos de personas naturales.
- Consecuencias de la denegación de servicio.
- Perdida o cifrado de información por malware
- Cualquier otro resultado generado producto del incidente

8.9 Incidentes en bases de datos de personas naturales

- Cuando el incidente es generado en el caso especial donde intervenga una base de datos de persona natural, es necesario realizar el registro del incidente en la página del registro nacional de bases de datos de la superintendencia de industria y comercio.
- (ii) **Incidentes de seguridad.** Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del Tratamiento o por su Encargado, que deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
- La información relacionada con las medidas de seguridad, los reclamos presentados por los Titulares y los incidentes reportados por los responsables del Tratamiento no estará disponible para consulta pública.

8.10 Área de sistemas de información

Se debe realizar una reunión junto con todos los afectados, donde se realizará un análisis de causas y efectos del incidente presentado, se debe establecer un plan de medidas preventivas y correctivas acompañados de un plan de gestión de cambios.
Posteriormente se establece un plan de capacitación y concientización de las nuevas medidas a aplicar y se completan todos los informes de análisis y de resultados.

9 Sistema de Gestión documental.

El alineamiento del sistema de protección de datos personales con el sistema de gestión documental corresponde al FONDO DE FOMENTO PANELERO y quedaron descritos en los entregables del mismo, la aplicabilidad de estos es responsabilidad del FONDO DE FOMENTO PANELERO, sin embargo, el sistema de protección de datos personales podrá realizar validaciones de forma autónoma y aleatoria con el fin de verificar que se implementen, ejecuten y cumplan.