

Kick Off

# Protección de Datos Personales

---

Noviembre, 2021



# Agenda



Introducción



Marco de trabajo



Organización del proyecto



Política Privacidad de la Información



Q&A

Thursday, December 2, 2021





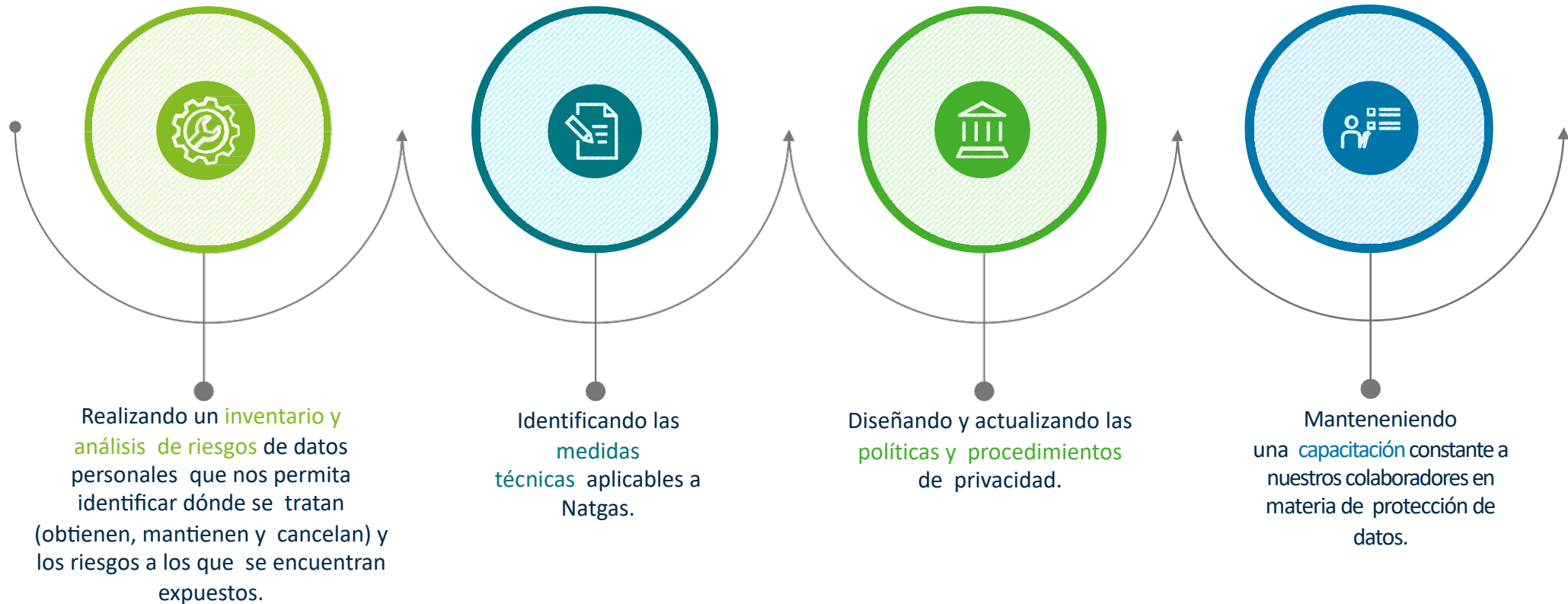
# Introducción

---



# Objetivo

Dar cumplimiento a los requerimientos de la LFPDPPP, su reglamento y demás normatividad aplicable.





# Marco de Trabajo

---



# Enfoque

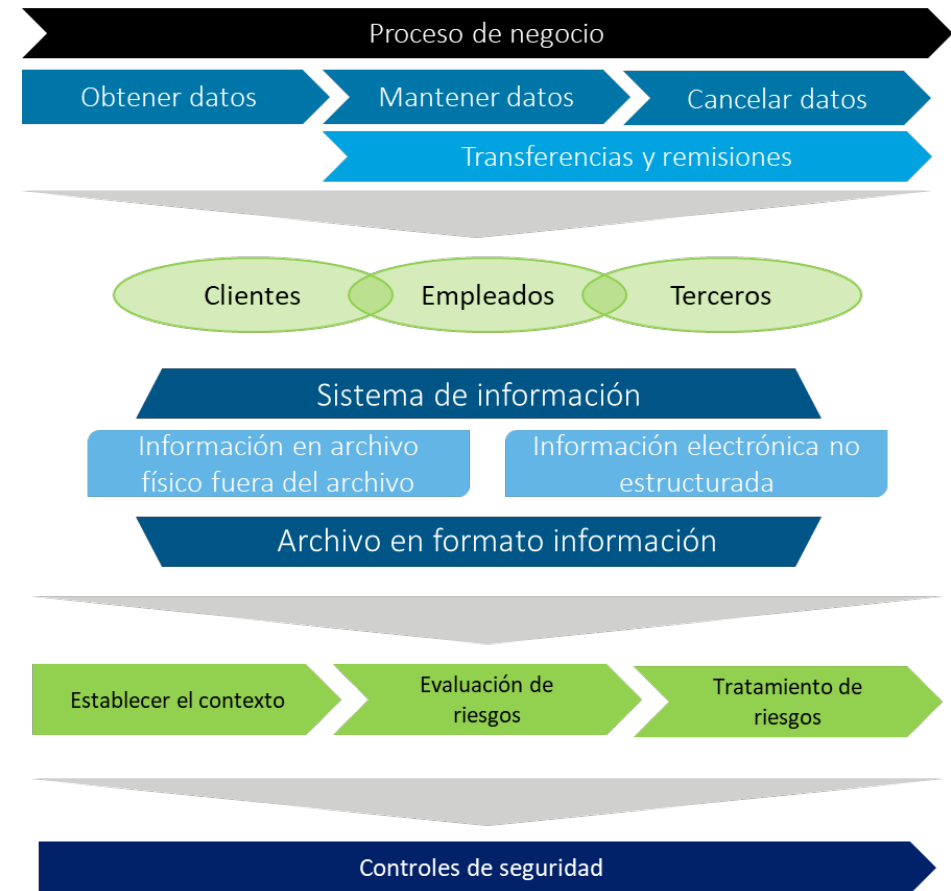
Dar cumplimiento a las leyes y regulaciones nacionales.

Los DP pueden ingresar a Natgas a través de diferentes procesos y por diversos medios.

Éstos atraviesan un tratamiento donde pueden ser: **usados, divulgados, almacenados, cancelados, resguardados o eliminados.**

Debemos tener claro ¿dónde quedan esos DP en nuestra Organización?, ¿Quién tiene derecho a acceder a ellos?, ¿Qué tratamiento sufren?, etc.

## Cumplimiento a leyes de privacidad nacionales



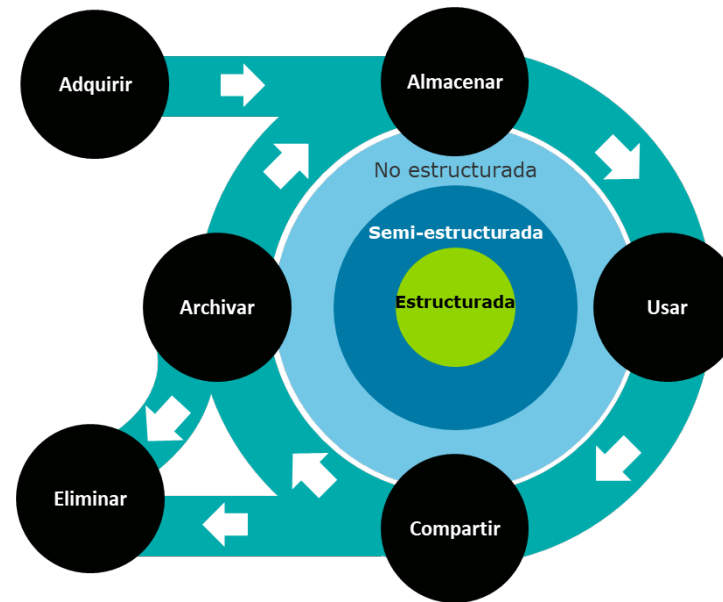


## Para una óptima implementación de controles, en Natgas debemos tener claridad de cómo gestionar el ciclo de vida de los datos...

El ciclo de vida de los DP:

- 1.- Adquirir
- 2.- Almacenar
- 3.- Usar
- 4.- Compartir
- 5.- Archivar
- 6.- Eliminar

Por cada área del negocio que maneje DP, se identificarán procesos clave y sus respectivos activos de información.

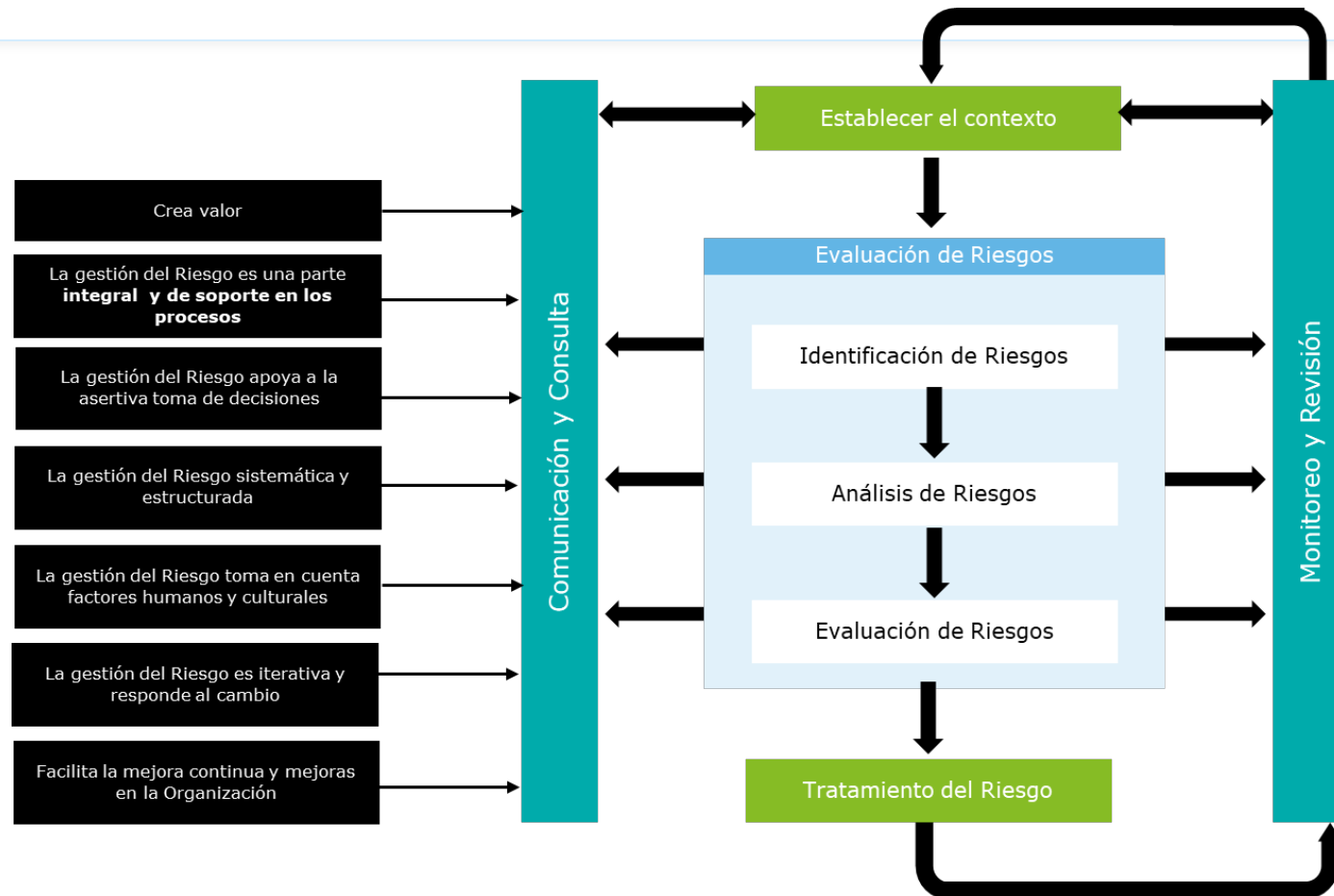


Con el uso de este enfoque podremos contestar las siguientes preguntas:

- ¿Cómo se crea la información? o ¿Quién crea la información?
- ¿Dónde se almacena la información?
- ¿Cómo se procesa la información?
- ¿Cómo se mantiene/trata/protege la información?
- ¿Cómo se elimina la información?
- Tiempos de retención y eliminación de la información.

La información existe en diversos formatos (físicos y digitales) y se dispersan a través de toda la organización y terceros. Los datos tienen un valor y riesgos que pueden variar por tipo y dependiendo de su etapa en el ciclo de vida.

Debemos también tener identificados los riesgos a los que puede estar expuesta nuestra organización...





# Organización del Proyecto

---



# Fases del proyecto



Fase 1

Planeación



Fase 2

Análisis



Fase 3

Diseño función de privacidad



Fase 4

Implementación

## Etapas

|                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1.1 Planeación</b> <ul style="list-style-type: none"> <li>Definir a los involucrados.</li> <li>Elaborar un plan de trabajo.</li> <li>Realizar la presentación de inicio del proyecto (Kick-Off / Entrenamiento FP)</li> <li>Identificar procesos y personal clave de las áreas de negocio que utilizan datos personales.</li> <li>Enviar el requerimiento de información.</li> <li>Elaborar agenda de entrevistas.</li> </ul> | <b>2.1 Inventario de datos personales</b> <ul style="list-style-type: none"> <li>Realizar el análisis de flujo de los datos personales.</li> <li>Identificar finalidades o actividades de procesamiento.</li> </ul>                                   | <b>3.1 Diseño función de privacidad</b> <ul style="list-style-type: none"> <li>Diseñar la siguiente documentación: <ul style="list-style-type: none"> <li>Estructura de privacidad</li> <li>Roles y responsabilidades de la estructura de privacidad</li> <li>Roles y responsabilidades como responsables y encargados de datos</li> </ul> </li> </ul> | <b>4.1 Documentación</b> <ul style="list-style-type: none"> <li>Medios de consentimiento</li> <li>Procesos de derechos de titulares.</li> <li>Políticas y procedimientos de privacidad</li> </ul> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>2.2 Análisis de riesgos y brechas</b> <ul style="list-style-type: none"> <li>Realizar el análisis de riesgos.</li> <li>Realizar el análisis de brechas de medidas jurídicas, administrativas y técnicas (seguridad de datos personales)</li> </ul> |                                                                                                                                                                                                                                                                                                                                                        | <b>4.2 Capacitación</b> <ul style="list-style-type: none"> <li>Capacitar al personal en materia de privacidad</li> </ul>                                                                          |

## Entregables

|                                                                                                                                |                                                                                                                                                                                                                                       |                                                                                                                                                                                          |                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Plan de trabajo detallado.</li> <li>Presentación de Kick-off / Entrenamiento</li> </ul> | <ul style="list-style-type: none"> <li>Inventario de datos personales</li> <li>Análisis de riesgos de datos personales.</li> <li>Análisis de brechas jurídicas, administrativas y técnicas (seguridad de datos personales)</li> </ul> | <ul style="list-style-type: none"> <li>Estructura de Privacidad con roles y responsabilidades de privacidad</li> <li>Documento de formalización del responsable de Privacidad</li> </ul> | <ul style="list-style-type: none"> <li>Procesos de atención de derechos</li> <li>Políticas y procedimientos de privacidad</li> <li>Material de capacitación</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



# Plan de trabajo

|     |                                | Mes 1 |   |   |   | Mes 2 |   |   |   |
|-----|--------------------------------|-------|---|---|---|-------|---|---|---|
|     |                                | 1     | 2 | 3 | 4 | 5     | 6 | 7 | 8 |
| 1.1 | Planeación                     |       |   |   |   |       |   |   |   |
| 2.1 | Inventario de datos personales |       |   |   |   |       |   |   |   |
| 2.2 | Análisis de riesgos y brechas  |       |   |   |   |       |   |   |   |
| 3.1 | Diseño                         |       |   |   |   |       |   |   |   |
| 4.1 | Documentación                  |       |   |   |   |       |   |   |   |
| 4.2 | Capacitación                   |       |   |   |   |       |   |   |   |



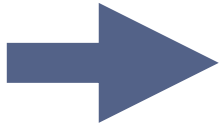
# Política de Protección de Datos Personales

---



# OBJETIVOS Y ALCANCE

A) Cumplir con cada uno de los **principios que establece la LFPDPPP** con respecto al tratamiento de datos personales:



- |                                |                                  |
|--------------------------------|----------------------------------|
| 1. Principio de licitud        | 5. Principio de calidad          |
| 2. Principio de lealtad        | 6. Principio de proporcionalidad |
| 3. Principio de consentimiento | 7. Principio de finalidad        |
| 4. Principio de información    | 8. Principio de responsabilidad  |

B) **Garantizar la seguridad de los datos personales** tratados en el interior de NATGAS

C) **Asegurar los correctos niveles de confidencialidad** de la información, así como la integridad

D) Aplica para **todo responsable que lleve a cabo tratamiento de datos personales** en sus procedimientos

# ¿EN QUÉ CONSISTE LA POLÍTICA?

1.- El cumplimiento de todos los principios que establece el artículo 6 de la LFPDPPP: **licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad**:



- a) Tratar y recabar datos personales de manera lícita
- b) Sujetar el tratamiento de datos personales al consentimiento del titular
- c) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines a través del aviso de privacidad
- d) Procurar que los datos personales tratados sean correctos y actualizados
- e) Suprimir los datos personales cuando hayan dejado de ser necesarios



# ¿EN QUÉ CONSISTE LA POLÍTICA?

- f) Tratar datos personales estrictamente el tiempo necesario
- g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad
- h) No obtener los datos personales a través de medios fraudulentos
- i) Respetar la expectativa razonable de privacidad del titular
- j) Tratar los menos datos personales posibles, y sólo aquellos que resulten necesarios

# ¿EN QUÉ CONSISTE LA POLÍTICA?

- 1.- Establecer y mantener medidas de seguridad de los datos personales
- 2.- Guardar la confidencialidad de los datos personales
- 3.- Identificar el flujo y ciclo de vida de los datos personales:
  - ✓ ¿por qué medio se recaban?
  - ✓ ¿en qué procesos de NATGAS se utilizan?
  - ✓ ¿con quién se comparten?
  - ✓ ¿en qué momento y por qué medios se suprimen?
- 4.- Mantener un inventario actualizado de los datos personales que maneja NATGAS
- 5.- Respetar los derechos de los titulares en relación con sus datos personales



# TIPOS DE DATOS PERSONALES

## DATOS PERSONALES SENSIBLES

Datos que afecten a la esfera más íntima de su titular:

- ✓ origen racial o étnico
- ✓ estado de salud pasado, presente y futuro
- ✓ información genética
- ✓ creencias religiosas, filosóficas y morales
- ✓ afiliación sindical
- ✓ opiniones políticas
- ✓ preferencia sexual
- ✓ hábitos sexuales

## DATOS PATRIMONIALES

Datos que permitan inferir el patrimonio de una persona:

- ✓ saldos bancarios
- ✓ estados y/o número de cuenta
- ✓ cuentas de inversión
- ✓ bienes muebles e inmuebles
- ✓ información fiscal
- ✓ historial crediticio
- ✓ ingresos y egresos
- ✓ buró de crédito
- ✓ seguros
- ✓ AFORES
- ✓ Fianzas
- ✓ no. tarjeta de crédito y/o débito

## DATOS DE AUTENTICACIÓN

Datos que permitan acreditar al titular:

- ✓ contraseñas
- ✓ información biométrica
- ✓ firma autógrafa y electrónica

Dentro de esta categoría se toman en cuenta los datos jurídicos tales como:

- ✓ antecedentes penales
- ✓ amparos
- ✓ demandas
- ✓ contratos
- ✓ litigios

# PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

## Principio de Licitud:

Los datos personales deberán ser recabados y tratados de manera lícita conforme a las disposiciones establecidas por la legislación mexicana y el derecho internacional: sin engaños, fraudes o medios ilícitos

## Principio de Consentimiento:

Los datos personales serán tratados únicamente cuando se haya obtenido de manera previa el consentimiento de su titular para el tratamiento de estos.

## Principio de Información:

Garantizar el derecho del titular a conocer quién trata su información personal y con qué fines (avisos de privacidad)

## Principio de Calidad:

Aplicar, desarrollar y hacer cumplir los procedimientos y mecanismos necesarios para procurar que los datos personales sean exactos, completos, correctos y actualizados.



# PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

## Principio de Finalidad:

Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad

## Principio de Lealtad:

No hacer uso de medios engañosos o fraudulentos para recabar y tratar datos personales

## Principio de Proporcionalidad:

El tratamiento de datos personales será necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad

## Principio de Responsabilidad:

Velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión.

## PRINCIPIO DE LICITUD

# TRATAMIENTO Y OBTENCIÓN LÍCITA DE DATOS PERSONALES

- ✓ Garantizar que los datos personales sean obtenidos de manera personal del titular por medio de las solicitudes, formatos físicos/ electrónicos, procedimientos aprobados por NATGAS; o bien cuando el titular los proporcione de manera presencial
- ✓ En caso de que NATGAS verifique que ha existido engaño y/o fraude en la obtención de los datos personales, se compromete a realizar las acciones disciplinarias en contra del personal responsable





## ¿CÓMO CUMPLIR CON EL PRINCIPIO DE LICITUD?

1. No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales
2. Respetar en todo momento la privacidad de los titulares, privilegiando su protección en el tratamiento de sus datos personales

## PRINCIPIO DE CONSENTIMIENTO

# OBTENCIÓN DEL CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

1. La solicitud del consentimiento deberá ir referida a una finalidad determinada en el aviso de privacidad
2. Cuando los datos personales se obtengan personalmente, el consentimiento deberá ser previo al tratamiento
3. Los datos financieros o patrimoniales sólo se obtendrán mediante el consentimiento expreso del titular
4. Para el tratamiento de datos personales sensibles, se deberá obtener el consentimiento expreso y por escrito del titular
5. El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos







## PRINCIPIO DE CONSENTIMIENTO

## CARACTERÍSTICAS DEL CONSENTIMIENTO

La obtención del consentimiento tácito o expreso deberá de cumplir con las siguientes características:

- ✓ **Libre:** sin que medie error, mala fe, violencia o dolo
- ✓ **Específica:** referida a una o varias finalidades determinadas que justifiquen el tratamiento
- ✓ **Informada:** que el titular tenga conocimiento del aviso de privacidad previo al tratamiento de sus datos personales



## ¿CÓMO CUMPLIR CON EL PRINCIPIO DE CONSENTIMIENTO?

1. Solicitar el consentimiento siempre ligado a finalidades específicas (aviso de privacidad)
2. Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito
3. Solicitar el consentimiento expreso para los datos personales financieros o patrimoniales, y el expreso y por escrito para los datos personales sensibles
4. Dar a conocer el Aviso de Privacidad previo a la obtención del consentimiento

## ¿CÓMO CUMPLIR CON EL PRINCIPIO DE CONSENTIMIENTO?

5. Implementar medios sencillos y gratuitos para la obtención del consentimiento
6. Llevar un control de los titulares que negaron su consentimiento y de las finalidades concretas para las cuales no se podrán tratar sus datos
7. Generar pruebas para acreditar que se cumplió con el principio de consentimiento (\*Auditorías)
8. Solicitar el consentimiento si hubo cambio en las finalidades informadas en el aviso de privacidad

# PRINCIPIO DE INFORMACIÓN

## AVISO DE PRIVACIDAD

Informar a los titulares sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

El aviso de privacidad deberá ser:

- ✓ sencillo
- ✓ información necesaria
- ✓ expresado en español
- ✓ lenguaje claro y comprensible
- ✓ estructura y diseño que facilite su entendimiento





## PRINCIPIO DE INFORMACIÓN

## AVISO DE PRIVACIDAD

Para ello, en el aviso de privacidad de NATGAS considera lo siguiente:

- A. No se usarán frases inexactas, ambiguas o vagas
- B. Tomar en cuenta para su redacción los perfiles de los titulares
- C. No incluir textos o formatos que induzcan al titular a elegir una opción en específico
- D. En caso de que se incluyan casillas para que el titular otorgue su consentimiento, no se deberán marcar previamente
- E. No remitir a textos o documentos que no estén disponibles para el titular



## PRINCIPIO DE INFORMACIÓN

## AVISO DE PRIVACIDAD MEDIOS DE DIFUSIÓN

Los avisos de privacidad podrán difundirse o reproducirse en cualquiera de los siguientes medios:

- ✓ formato físico
- ✓ electrónico
- ✓ óptico
- ✓ sonoro
- ✓ visual
- ✓ a través de cualquier otra tecnología que permita su eficaz comunicación

El aviso de privacidad se pondrá a disposición del titular en los siguientes momentos:

- ✓ Cuando los datos personales se obtengan de manera directa del titular, se pondrá a su disposición el aviso de privacidad previo a la obtención de los mismos
- ✓ Cuando los datos personales se obtengan de manera indirecta de su titular; o bien, de una fuente de acceso público, se pondrá a disposición el aviso de privacidad al primer contacto con el titular
- ✓ Cuando los datos personales se traten para una finalidad distinta a la consentida por el titular, se pondrá a su disposición un nuevo aviso de privacidad con las características del nuevo tratamiento



## ¿CÓMO CUMPLIR CON EL PRINCIPIO DE INFORMACIÓN?

- ✓ Conservar el aviso de privacidad con el consentimiento otorgado por el titular, para acreditar que se obtuvo el consentimiento por parte del mismo
- ✓ Disponibilidad del aviso de privacidad en los medios donde se recaban los datos personales
- ✓ Verificar que los medios en los que se difunde y pone a disposición el aviso de privacidad sean de acceso gratuito
- ✓ Inclusión del aviso de privacidad en el portal de Internet

# TRATAMIENTO DE DATOS CORRECTOS Y ACTUALIZADOS

1. Procedimientos para corregir y actualizar los datos personales en atención al ejercicio de derechos ARCO
2. Procedimientos para corregir y actualizar los datos personales cuando se cuenta con evidencia que demuestra que los mismos son incorrectos y/o inexactos
3. Se realizan campañas de actualización de los datos personales, dirigidas a los titulares
4. Se informa a los encargados, sobre las correcciones o actualizaciones de los datos personales
5. Se incluyen cláusulas contractuales en los contratos que se firmen con terceros que tratan datos personales
6. Se definen plazos de bloqueo y conservación de los datos personales
7. Se establecen procedimientos seguros para la destrucción de los datos personales

# OBTENCIÓN DE DATOS

## DE MANERA PERSONAL DEL TITULAR

Obtener los datos personales por medio de las solicitudes y/o formatos aprobados por NATGAS o bien cuando el titular los proporcione de manera presencial

## DE MANERA PRESENCIAL

Previo a la obtención de los datos, se realizará una acreditación de la identidad del titular, cotejando los documentos exhibidos con sus originales y verificando que la persona que proporciona los datos para el trámite sea el titular o una persona legalmente autorizada por él.

## FORMATOS Y/O SOLICITUDES EN FORMATO FÍSICO

En caso de que el titular llene una solicitud en formato físico o ésta sea llenada por personal de NATGAS, se deberá de verificar que los datos personales asentados en la solicitud sean aquellos que el titular proporciona

# SUPRESIÓN DE LOS DATOS PERSONALES

## Documentación soporte papel:

- ✓ Los documentos existentes en papel que contengan datos personales de NATGAS, están prohibidos tirarlos a la basura, sin previamente destruirlos con las trituradoras de papel (corte en tirad o cruzado)
- ✓ Queda prohibido deshacerse de la documentación impresa mediante su depósito en papeleras, contenedores o bolsas de basura
- ✓ Deben destruirse las copias o reproducciones desechadas

# SUPRESIÓN DE LOS DATOS PERSONALES

## **Destrucción de información en soportes electrónicos:**

Los medios eficaces que sigue NATGAS son: la desmagnetización y la sobre-escritura

**A.Desmagnetización:** exposición de los soportes de almacenamiento a un potente campo magnético; proceso que elimina los datos almacenados en el dispositivo.

**B. Sobre-escritura:** se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados



# TRATAMIENTO DE DATOS PERSONALES ESTRICTAMENTE DURANTE EL TIEMPO NECESARIO

1. Ningún dato personal debe continuar bajo tratamiento una vez cumplidas las finalidades para las que fue recabado
2. Una vez que los datos personales ya no sean necesarios, se debe proceder a la cancelación de los datos, previo bloqueo de los mismos, para su posterior supresión.
3. La cancelación es el procedimiento de cesar el uso de los datos. La cancelación implicará el bloqueo de los datos, con el fin de impedir su tratamiento
4. Durante el periodo de bloqueo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación
5. Los plazos en los que no se pueden suprimir los datos, por el posible acontecimiento de que alguna autoridad requiriera de NATGAS la información, son los siguientes:

Laboral: 2 años

Fiscal: 5 años

Mercantil: 10 años

Administrativo: 3 años

# LIMITACIÓN DEL TRATAMIENTO DE LOS DATOS PERSONALES



- Cumplir con los parámetros para elaborar un aviso de privacidad
- Inclusión de cláusulas en los contratos que se firman con terceros
- Capacitación al personal para que conozca la forma en que deben tratarse los datos conforme a lo señalado en el aviso de privacidad

# NO OBTENCIÓN DE DATOS A TRAVÉS DE MEDIOS FRAUDULENTOS

- A. Revisión de los procedimientos y formatos utilizados por NATGAS y por los encargados contratados para recabar datos personales.
- B. Se prevén sanciones para el personal o encargados en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales como son la rescisión contractual y medidas disciplinarias.



# TRATAMIENTO DE LOS DATOS MÍNIMOS POSIBLES

1. Se identifican las finalidades del tratamiento de los datos personales y los datos personales necesarios para cumplir con la finalidad principal
2. Se incluyen cláusulas en materia de protección de datos personales con terceros
3. Se realizan reducciones a los tratamientos detectados y se eliminan de las bases de datos aquéllos que no son indispensables
4. Se verifica cuál es el periodo que se requieren conservar los datos personales sensibles, y una vez transcurrido se eliminan
5. Se verifica que el tratamiento de datos sensibles atienda a cada una de las reglas antes precisadas

# VELAR POR EL CUMPLIMIENTO DE LOS PRINCIPIOS

1. En los contratos celebrados con empleados, encargados y/o terceros, se incluyen cláusulas en las que se comprometan a garantizar el adecuado tratamiento de los datos personales
2. Se establecen acciones técnicas y administrativas para la protección de los datos personales
3. Se adoptan políticas de privacidad
4. Se establecen programas de capacitación, concientización y actualización de datos personales
5. Se analizan los riesgos del tratamiento de datos personales
6. Se documenta por medio de contratos la comunicación del aviso de privacidad a terceros

# MEDIDAS DE SEGURIDAD

1. Inventario de datos personales y de los sistemas de tratamiento
2. Identificación de funciones y obligaciones de las personas que traten datos personales
3. Análisis de riesgos de datos personales
4. Plan de trabajo para la implementación de la Política de Seguridad de Datos Personales
5. Revisiones y/o auditorías a todas las áreas que tratan datos personales
6. Capacitación al personal que efectúa el tratamiento de datos personales
7. Registro de los medios de almacenamiento de los datos personales



# DEBER DE CONFIDENCIALIDAD

- A. Se establecen procedimientos para evitar fuga de información o el acceso indebido a los datos personales
- B. Se capacita al personal para que conozca sus obligaciones con relación al tratamiento de datos personales
- C. Se incluyen cláusulas de confidencialidad en los contratos con empleados y terceros que tratan datos personales
- D. Se realizan verificaciones periódicas a los encargados del tratamiento a fin de que cumplan con las obligaciones

# INVENTARIO DE DATOS PERSONALES

Información básica que permite conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su flujo o ciclo de vida, considerando:

- Obtención
- Almacenamiento
- Uso
  - Acceso
  - Manejo
  - Aprovechamiento
  - Monitoreo
  - Procesamiento (incluidos los sistemas que se utilizan para tal fin)
- Divulgación
  - Remisiones
  - Transferencias
- Bloqueo
- Cancelación, supresión o destrucción

El inventario de datos personales se desarrollará de acuerdo a una clasificación de los datos personales por niveles de seguridad y de acuerdo a las categorías de información

# CATEGORÍAS DE INFORMACIÓN

## A.- INFORMACIÓN PERSONAL

Cualquier información concerniente a una persona física identificada o identificable:

- a. Datos de identificación
- b. Datos de contacto
- c. Datos académicos
- d. Datos laborales
- e. Datos patrimoniales
- f. Datos financieros
- g. Datos sensibles
- h. Datos de menores de edad
- i. Datos de terceros

## B.- INFORMACIÓN PERSONAL SENSIBLE

Aquellos datos que afecten a la esfera más íntima de su titular:

- a. origen racial o étnico
- b. estado de salud pasado, presente y futuro
- c. información genética
- d. creencias religiosas, filosóficas y morales
- e. afiliación sindical
- f. opiniones políticas
- g. preferencia sexual
- h. hábitos sexuales

# NIVELES DE SEGURIDAD

Se deberá de clasificar la información tratada atendiendo a los siguientes niveles de seguridad:

## NIVEL ESTANDAR

Información de identificación, contacto, datos laborales y académicos, tal como:

- nombre
- teléfono
- edad
- sexo
- RFC
- CURP
- estado civil
- correo electrónico
- lugar y fecha de nacimiento,
- nacionalidad
- puesto de trabajo
- lugar de trabajo
- experiencia laboral
- datos de contacto laborales
- idioma o lengua
- escolaridad
- trayectoria educativa
- títulos
- certificados
- cédula profesional
- entre otros

## NIVEL SENSIBLE

Datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país.

- Datos patrimoniales
- Datos de autenticación
- Datos sensibles

## NIVEL ESPECIAL

Son los que de acuerdo a su naturaleza y contexto pueden causar un daño excepcional a los titulares:

- Información adicional de tarjeta de crédito
- Datos personales de titulares de alto riesgo: cuya profesión, oficio o condición los expone a una mayor probabilidad de ser atacados debido al beneficio económico o reputación
- Impartición de justicia y seguridad nacional: cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional

# CONSECUENCIAS EN CASO DE INCUMPLIMIENTO

En caso de incurrir en alguno(s) de los supuestos contenidos en la presente política; el responsable se hará acreedor a las sanciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Se consideran como incumplimiento a la protección de datos personales, las siguientes:

1. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales
2. Actuar con negligencia o dolo
3. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente política
4. Incumplir el deber de confidencialidad establecido en la Ley
5. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos
6. Vulnerar la seguridad de bases de datos
7. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley
8. Recabar o transferir datos personales sin el consentimiento expreso del titular
9. Recabar datos en forma engañosa y fraudulenta