PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

DIRECCIÓN NACIONAL EXTRAORDINARIA

PROYECTO DE ACTA DE SESIÓN: 04/EXT/16-04-2020

En la Ciudad de México, siendo las dieciocho horas del día dieciséis de abril del dos mil veinte, mediante video llamada de *Whatsapp*; en atención a la convocatoria generada el 14 de abril del año dos mil veinte, notificada por correo electrónico a los integrantes del Comité de Transparencia del Partido de la Revolución Democrática, en los términos de la *SEGUNDA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA*, para celebrar la **CUARTA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.**

Se reunieron los siguientes ciudadanos: -

Antonio Aarón Ávalos de Anda	**Presidente del Comité de Transparencia del Partido de la Revolución Democrática.**
Tania Maratalina Roque Medel	**Integrante de la Unidad de Transparencia del Partido de la Revolución Democrática.**
Salvador González García	**Integrante del Comité de Transparencia del Partido de la Revolución Democrática.**

Antonio Aarón Ávalos de Anda, manifestó, buenas tardes, dado que, además del de la voz, se cuenta con la presencia de Salvador González García, integrante del Comité de Transparencia del Partido de la Revolución Democrática, se declara la existencia del *Quórum* legal, por lo que se dio por cumplido el **punto 1** del orden del día consistente en *"Verificación y declaración del Quórum Legal"*, procediendo al desahogo del **punto 2**, del orden del día consistente en *"Lectura y en su caso aprobación, del Orden del Día"*

"ORDEN DEL DÍA

1. *Verificación y declaración del Quórum Legal;*
2. *Lectura y aprobación, en su caso, del Orden del Día;*
3. *Análisis, discusión y en su caso aprobación del Documento de Seguridad del Partido de la Revolución Democrática; y*

4. *Clausura".*

Lo anterior se notifica, para los efectos legales y estatutarios a que haya lugar.

Acto seguido, el Presidente del Comité de Transparencia de este Instituto político manifestó: "De estar conformes los miembros del Comité de Transparencia presentes, con la aprobación del orden del día, sírvanse manifestarlo mediante votación económica."

Como resultado de lo anterior, se obtuvieron dos votos a favor, por lo tanto, se aprueba por unanimidad el orden del día.

Ahora bien, con relación al tercer punto del orden del día, se hace constar que previamente, la documentación fue circulada a los integrantes, por ello, se consulta a los integrantes de este Pleno, si están de conformidad con dispensar la lectura de dichos documentos, de ser así, por favor, sírvanse manifestarlo mediante manifestación económica.

Al computarse dos votos a favor se tiene por aprobada la moción por unanimidad.

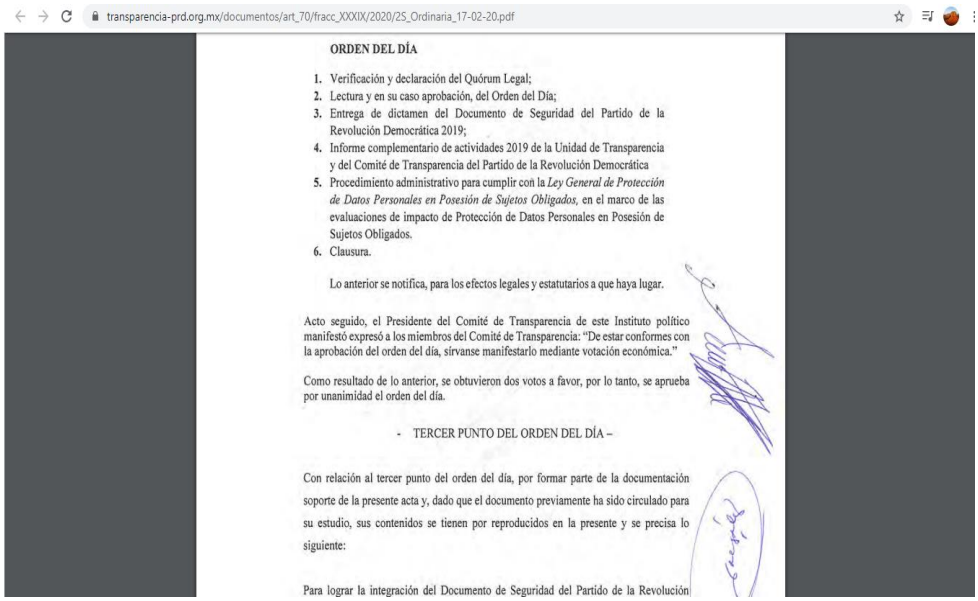
Ahora bien, el de la voz, advierte que la Unidad de Transparencia del Partido de la Revolución Democrática, en el ejercicio de sus atribuciones, tuvo a bien generar un instrumento de transparencia proactiva intitulado *Informe sobre el Documento de Seguridad en Materia de Protección de Datos Personales del Partido de la Revolución Democrática*, mismo que fue presentado a este Comité de Transparencia con la finalidad de valorar su contenido y, poder determinar si cumple con las características que debe tener el *Documento de Seguridad del Partido de la Revolución Democrática*[1], por ello, este Comité de Transparencia, procede a valorar sus contenidos, con base en los siguientes:

[1] https://transparencia-prd.org.mx/documentos/art_70/fracc_XLVIII/TransparenciaProactiva_DS_PRD_2019-2020.pdf

RESULTANDOS

Con fecha 14 de abril de dos mil veinte, fue remitido por la Secretaría Técnica de este Comité, documento intitulado *"Informe sobre el Documento de Seguridad en materia de Protección de Datos Personales del Partido de la Revolución Democrática",* en los siguientes términos:

> *"El documento de seguridad del Partido de la Revolución Democrática, ha sido generado a partir del trabajo conjunto entre la Unidad y el Comité de Transparencia del Partido de la Revolución Democrática, en el ámbito de sus facultades y atribuciones, así como los instrumentos que cada órgano intrapartidario de este Instituto político generaron. Se concibe como la suma de dichos instrumentos y dan pie a la elaboración de este informe, que busca integrar, de manera general, todas las manifestaciones y posicionamientos que fueron remitidos a la Unidad de Transparencia del PRD, para facilitar a la sociedad, a través de la transparencia proactiva, un producto integrador que explique los términos en que este Partido político ha integrado su Documento de Seguridad en Materia de Protección de Datos Personales.*
>
> *El artículo 35 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, establece que todo Sujeto Obligado, en este caso, el Partido de la Revolución Democrática, debe contar con un documento de seguridad, que conforme a la fracción XIV del artículo 3° de esa ley general, es: "un instrumento que describe y da cuenta de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Sujeto Obligado para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee."*
>
> *Ahora bien, tomando en cuenta que durante la Segunda Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática celebrada el diecisiete de febrero del año dos mil veinte, se aprobó el Dictamen del Documento de Seguridad del Partido de la Revolución Democrática 2019, como se puede observar mediante el siguiente hipervínculo, https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2020/2S_Ordinaria_17-02-20.pdf, se provee evidencia documental:*



transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2020/2S_Ordinaria_17-02-20.pdf

ORDEN DEL DÍA

1. Verificación y declaración del Quórum Legal;
2. Lectura y en su caso aprobación, del Orden del Día;
3. Entrega de dictamen del Documento de Seguridad del Partido de la Revolución Democrática 2019;
4. Informe complementario de actividades 2019 de la Unidad de Transparencia y del Comité de Transparencia del Partido de la Revolución Democrática
5. Procedimiento administrativo para cumplir con la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,* en el marco de las evaluaciones de impacto de Protección de Datos Personales en Posesión de Sujetos Obligados.
6. Clausura.

Lo anterior se notifica, para los efectos legales y estatutarios a que haya lugar.

Acto seguido, el Presidente del Comité de Transparencia de este Instituto político manifestó expresó a los miembros del Comité de Transparencia: "De estar conformes con la aprobación del orden del día, sírvanse manifestarlo mediante votación económica."

Como resultado de lo anterior, se obtuvieron dos votos a favor, por lo tanto, se aprueba por unanimidad el orden del día.

- TERCER PUNTO DEL ORDEN DEL DÍA –

Con relación al tercer punto del orden del día, por formar parte de la documentación soporte de la presente acta y, dado que el documento previamente ha sido circulado para su estudio, sus contenidos se tienen por reproducidos en la presente y se precisa lo siguiente:

Para lograr la integración del Documento de Seguridad del Partido de la Revolución

Los contenidos de dicha sesión, se tienen por reproducidos en el presente instrumento, *así como lo dispuesto en los Avisos de Privacidad del Partido de la Revolución Democrática, sitos en su página principal: https://www.prd.org.mx/, se ofrecen capturas de pantalla:*

INICIO

prd.org.mx

Partido de la Revolución Democrática

INICIO DOCUMENTOS BOLETINES DE PRENSA SITIOS WEB TRANSPARENCIA

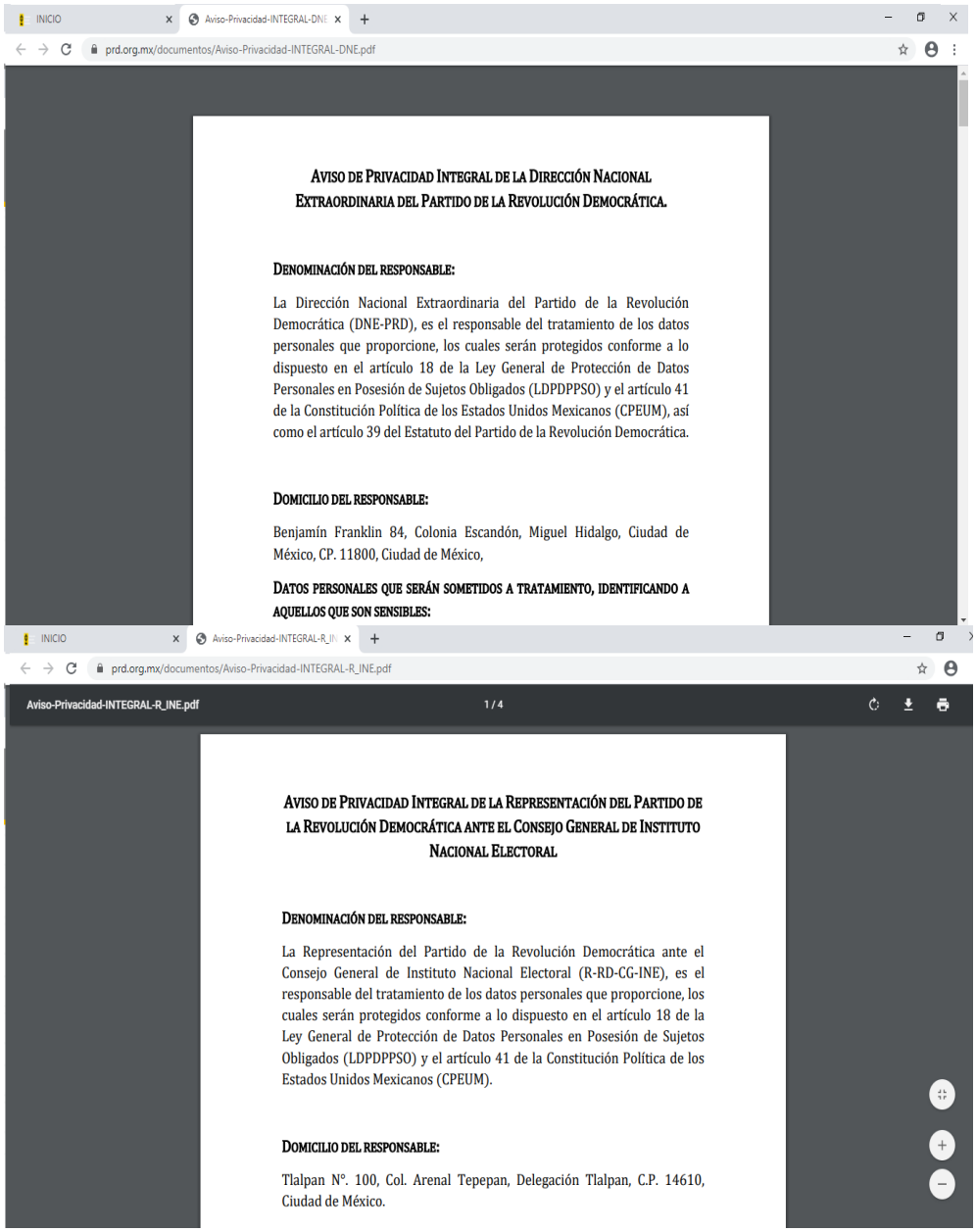
SENADO LXIV | Cámara de Diputados | Comités Estatales | Trabajamos para la Gente !!

Avisos de Privacidad del PRD

-Ley Federal del trabajo (Última Reforma DOF-02-07-2019)
Aviso de Privacidad Integral de la DNE
Aviso de Privacidad Integral de la representación del INE
-Aviso de Privacidad Integral Campaña nacional en defensa de la Salud
-Aviso de Privacidad Simplificado Campaña nacional en defensa de la salud
-Aviso de privacidad Integral del departamento de recursos Humanos e Informática del PRD
-Aviso de privacidad Integral de la Dirección Nacional de Comunicación del PRD
-Aviso de privacidad Integral del Órgano Técnico Electoral del PRD

Avisos de Privacidad del PRD

-Aviso de Privacidad Integral del Organo de Afiliación
-Aviso de privacidad del Departamento Jurídico de la Coordinación Nacional del Patrimonio y Recursos
-Aviso de Privacidad de Tesorería de la Coordinación Nacional del Patrimonio
-Departamento de Contabilidad de la Coordinación Nacional del Patrimonio y Recursos Financieros
-Aviso de Privacidad de la Unidad de Transparencia del PRD
-Aviso de Privacidad del Consejo Nacional del PRD
-Aviso de privacidad Integral del Instituto de Formación del PRD



AVISO DE PRIVACIDAD INTEGRAL DE LA DIRECCIÓN NACIONAL EXTRAORDINARIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

DENOMINACIÓN DEL RESPONSABLE:

La Dirección Nacional Extraordinaria del Partido de la Revolución Democrática (DNE-PRD), es el responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en el artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LDPDPPSO) y el artículo 41 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), así como el artículo 39 del Estatuto del Partido de la Revolución Democrática.

DOMICILIO DEL RESPONSABLE:

Benjamín Franklin 84, Colonia Escandón, Miguel Hidalgo, Ciudad de México, CP. 11800, Ciudad de México,

DATOS PERSONALES QUE SERÁN SOMETIDOS A TRATAMIENTO, IDENTIFICANDO A AQUELLOS QUE SON SENSIBLES:

Aviso-Privacidad-INTEGRAL-R_INE.pdf 1 / 4

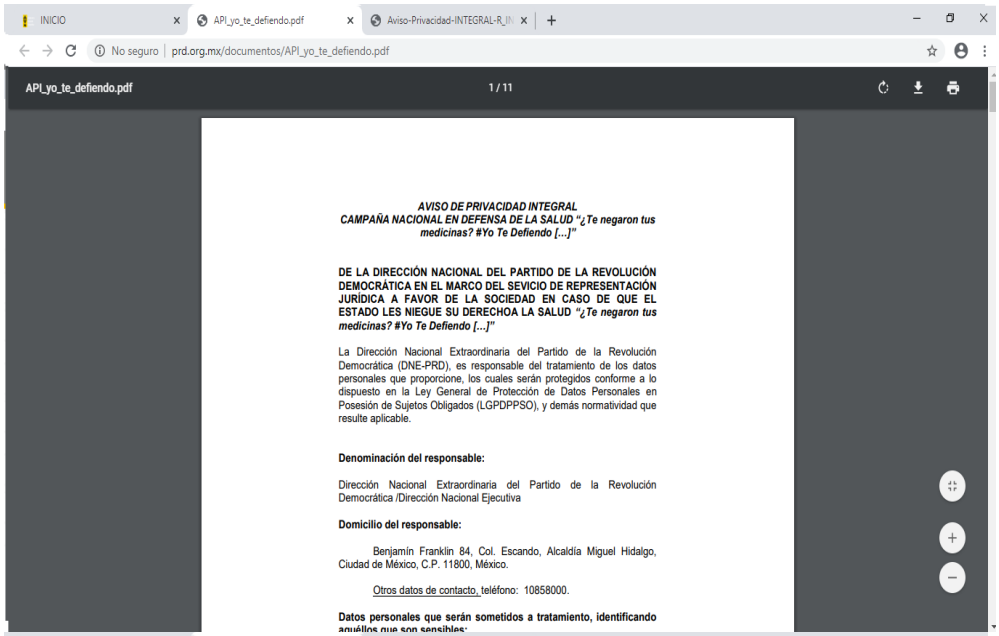
AVISO DE PRIVACIDAD INTEGRAL DE LA REPRESENTACIÓN DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA ANTE EL CONSEJO GENERAL DE INSTITUTO NACIONAL ELECTORAL

DENOMINACIÓN DEL RESPONSABLE:

La Representación del Partido de la Revolución Democrática ante el Consejo General de Instituto Nacional Electoral (R-RD-CG-INE), es el responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en el artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LDPDPPSO) y el artículo 41 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

DOMICILIO DEL RESPONSABLE:

Tlalpan N°. 100, Col. Arenal Tepepan, Delegación Tlalpan, C.P. 14610, Ciudad de México.



AVISO DE PRIVACIDAD INTEGRAL
CAMPAÑA NACIONAL EN DEFENSA DE LA SALUD "¿Te negaron tus medicinas? #Yo Te Defiendo […]"

DE LA DIRECCIÓN NACIONAL DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA EN EL MARCO DEL SEVICIO DE REPRESENTACIÓN JURÍDICA A FAVOR DE LA SOCIEDAD EN CASO DE QUE EL ESTADO LES NIEGUE SU DERECHOA LA SALUD *"¿Te negaron tus medicinas? #Yo Te Defiendo […]"*

La Dirección Nacional Extraordinaria del Partido de la Revolución Democrática (DNE-PRD), es responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y demás normatividad que resulte aplicable.

Denominación del responsable:

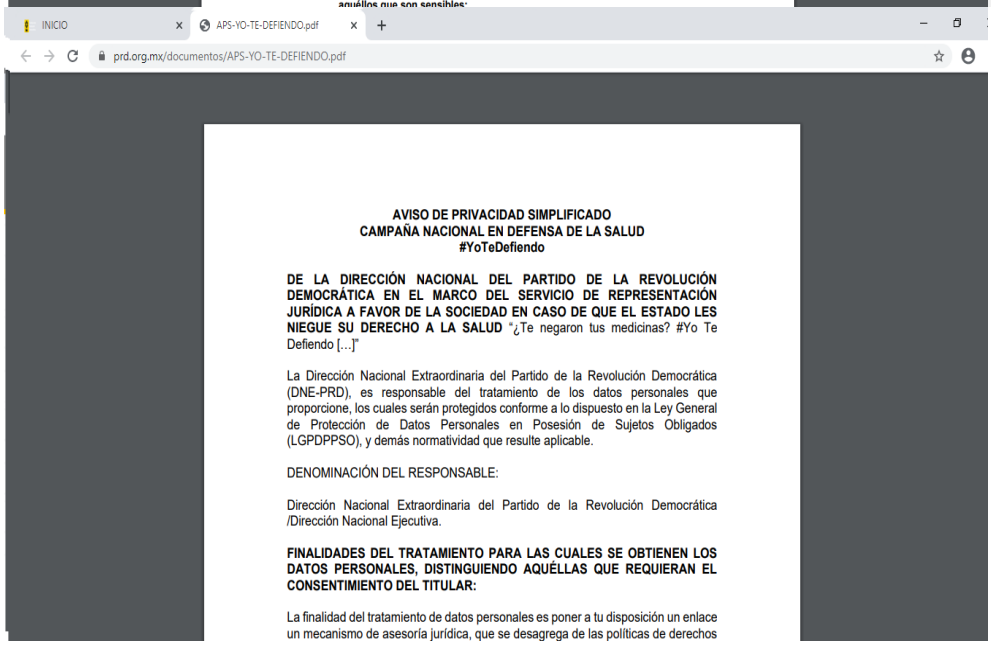
Dirección Nacional Extraordinaria del Partido de la Revolución Democrática /Dirección Nacional Ejecutiva

Domicilio del responsable:

Benjamín Franklin 84, Col. Escando, Alcaldía Miguel Hidalgo, Ciudad de México, C.P. 11800, México.

Otros datos de contacto, teléfono: 10858000.

Datos personales que serán sometidos a tratamiento, identificando



AVISO DE PRIVACIDAD SIMPLIFICADO
CAMPAÑA NACIONAL EN DEFENSA DE LA SALUD
#YoTeDefiendo

DE LA DIRECCIÓN NACIONAL DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA EN EL MARCO DEL SERVICIO DE REPRESENTACIÓN JURÍDICA A FAVOR DE LA SOCIEDAD EN CASO DE QUE EL ESTADO LES NIEGUE SU DERECHO A LA SALUD "¿Te negaron tus medicinas? #Yo Te Defiendo […]"

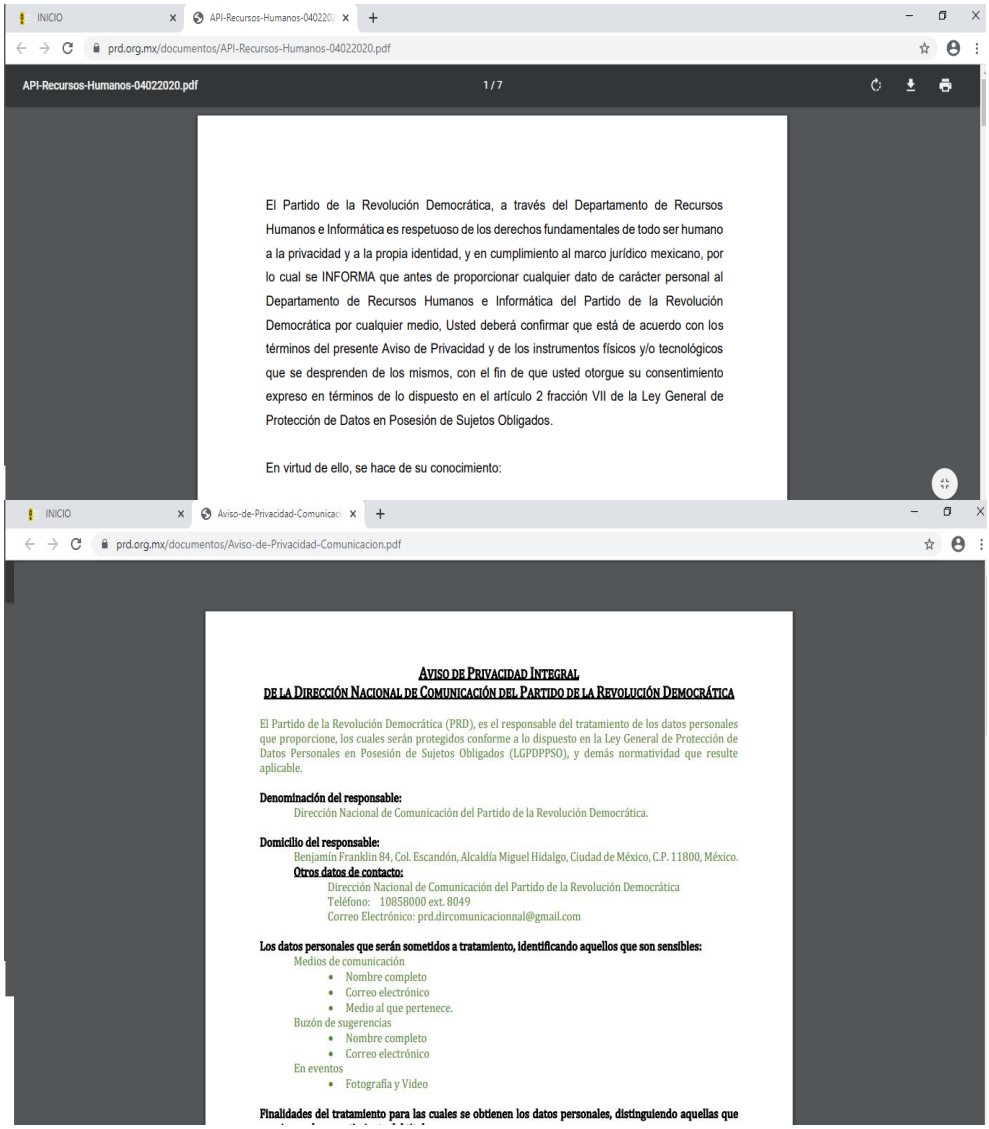
La Dirección Nacional Extraordinaria del Partido de la Revolución Democrática (DNE-PRD), es responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y demás normatividad que resulte aplicable.

DENOMINACIÓN DEL RESPONSABLE:

Dirección Nacional Extraordinaria del Partido de la Revolución Democrática /Dirección Nacional Ejecutiva.

FINALIDADES DEL TRATAMIENTO PARA LAS CUALES SE OBTIENEN LOS DATOS PERSONALES, DISTINGUIENDO AQUÉLLAS QUE REQUIERAN EL CONSENTIMIENTO DEL TITULAR:

La finalidad del tratamiento de datos personales es poner a tu disposición un enlace un mecanismo de asesoría jurídica, que se desagrega de las políticas de derechos



INICIO | API-Recursos-Humanos-040220 | prd.org.mx/documentos/API-Recursos-Humanos-04022020.pdf

API-Recursos-Humanos-04022020.pdf 1 / 7

El Partido de la Revolución Democrática, a través del Departamento de Recursos Humanos e Informática es respetuoso de los derechos fundamentales de todo ser humano a la privacidad y a la propia identidad, y en cumplimiento al marco jurídico mexicano, por lo cual se INFORMA que antes de proporcionar cualquier dato de carácter personal al Departamento de Recursos Humanos e Informática del Partido de la Revolución Democrática por cualquier medio, Usted deberá confirmar que está de acuerdo con los términos del presente Aviso de Privacidad y de los instrumentos físicos y/o tecnológicos que se desprenden de los mismos, con el fin de que usted otorgue su consentimiento expreso en términos de lo dispuesto en el artículo 2 fracción VII de la Ley General de Protección de Datos en Posesión de Sujetos Obligados.

En virtud de ello, se hace de su conocimiento:

INICIO | Aviso-de-Privacidad-Comunicaci | prd.org.mx/documentos/Aviso-de-Privacidad-Comunicacion.pdf

AVISO DE PRIVACIDAD INTEGRAL
DE LA DIRECCIÓN NACIONAL DE COMUNICACIÓN DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA

El Partido de la Revolución Democrática (PRD), es el responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y demás normatividad que resulte aplicable.

Denominación del responsable:
Dirección Nacional de Comunicación del Partido de la Revolución Democrática.

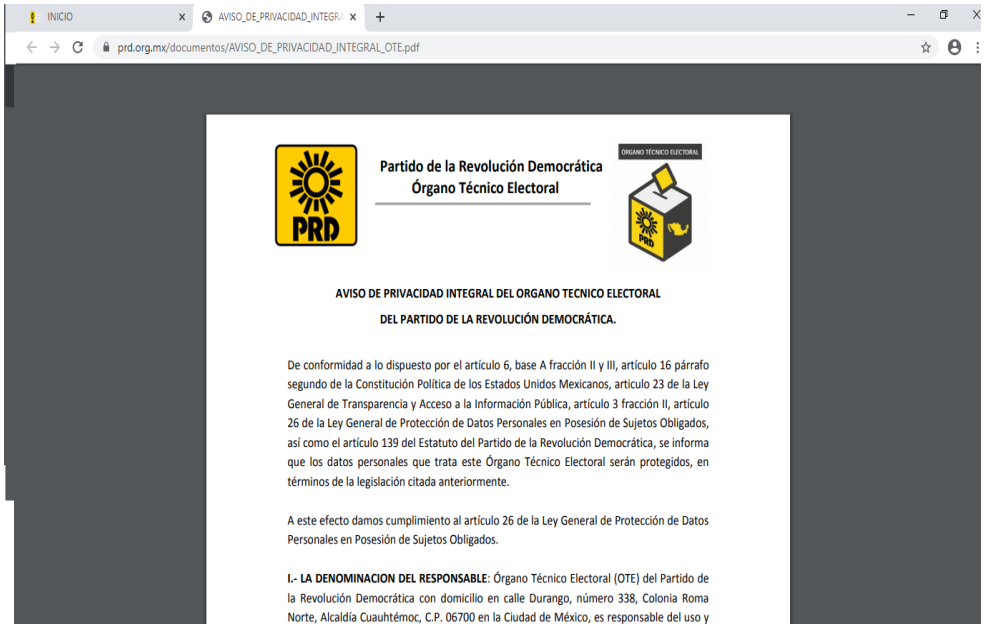
Domicilio del responsable:
Benjamín Franklin 84, Col. Escandón, Alcaldía Miguel Hidalgo, Ciudad de México, C.P. 11800, México.
Otros datos de contacto:
Dirección Nacional de Comunicación del Partido de la Revolución Democrática
Teléfono: 10858000 ext. 8049
Correo Electrónico: prd.dircomunicacionnal@gmail.com

Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles:
Medios de comunicación
- Nombre completo
- Correo electrónico
- Medio al que pertenece.

Buzón de sugerencias
- Nombre completo
- Correo electrónico

En eventos
- Fotografía y Video

Finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que



INICIO | AVISO_DE_PRIVACIDAD_INTEGRAL_OTE.pdf

prd.org.mx/documentos/AVISO_DE_PRIVACIDAD_INTEGRAL_OTE.pdf

Partido de la Revolución Democrática
Órgano Técnico Electoral

ÓRGANO TÉCNICO ELECTORAL

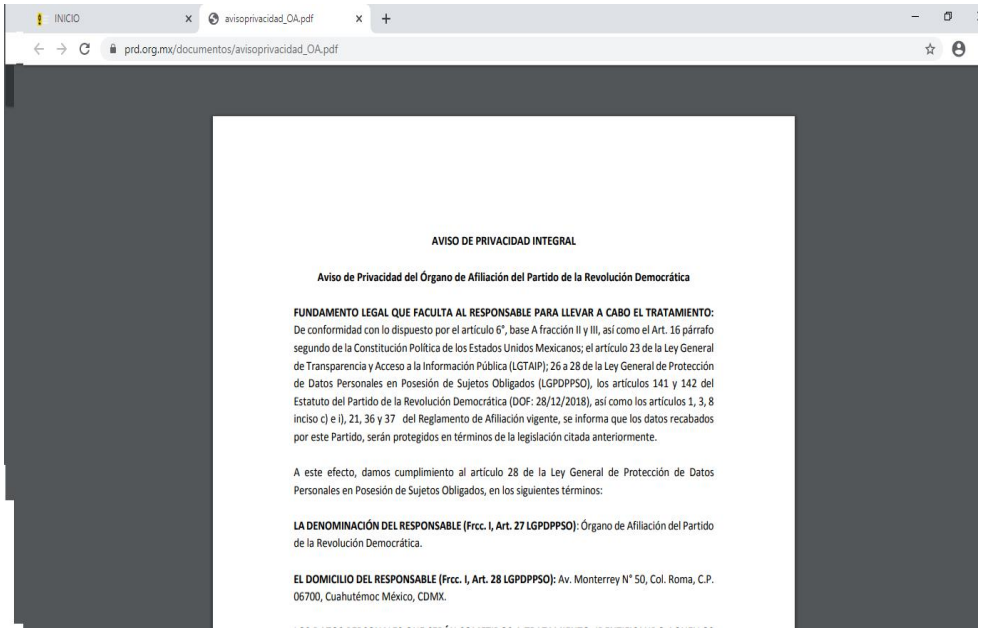
AVISO DE PRIVACIDAD INTEGRAL DEL ORGANO TECNICO ELECTORAL

DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

De conformidad a lo dispuesto por el artículo 6, base A fracción II y III, artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, articulo 23 de la Ley General de Transparencia y Acceso a la Información Pública, artículo 3 fracción II, artículo 26 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 139 del Estatuto del Partido de la Revolución Democrática, se informa que los datos personales que trata este Órgano Técnico Electoral serán protegidos, en términos de la legislación citada anteriormente.

A este efecto damos cumplimiento al artículo 26 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

I.- LA DENOMINACION DEL RESPONSABLE: Órgano Técnico Electoral (OTE) del Partido de la Revolución Democrática con domicilio en calle Durango, número 338, Colonia Roma Norte, Alcaldía Cuauhtémoc, C.P. 06700 en la Ciudad de México, es responsable del uso y



INICIO | avisoprivacidad_OA.pdf

prd.org.mx/documentos/avisoprivacidad_OA.pdf

AVISO DE PRIVACIDAD INTEGRAL

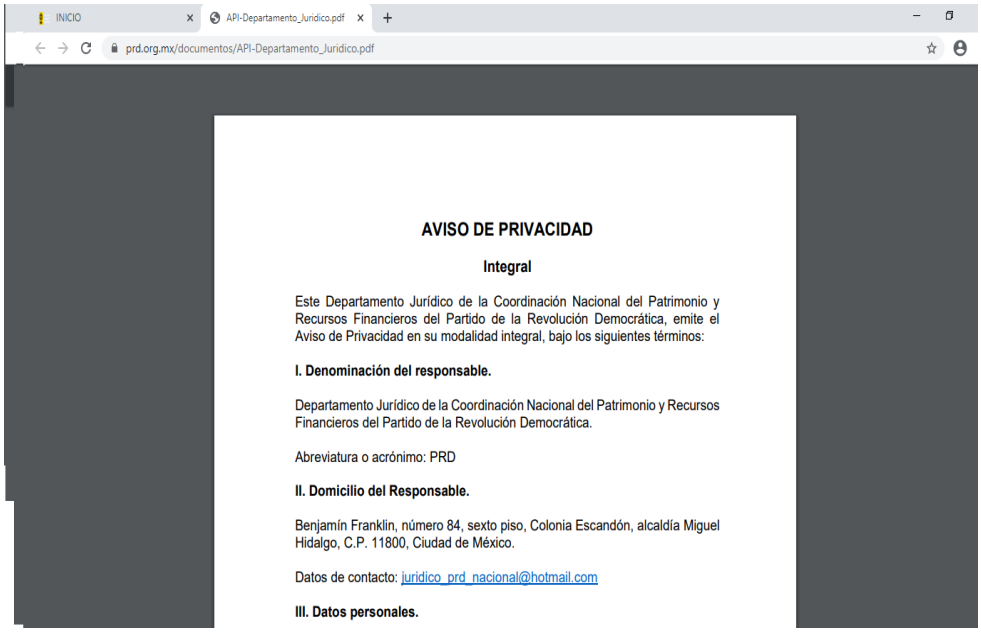
Aviso de Privacidad del Órgano de Afiliación del Partido de la Revolución Democrática

FUNDAMENTO LEGAL QUE FACULTA AL RESPONSABLE PARA LLEVAR A CABO EL TRATAMIENTO: De conformidad con lo dispuesto por el artículo 6°, base A fracción II y III, así como el Art. 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos; el artículo 23 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 26 a 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los artículos 141 y 142 del Estatuto del Partido de la Revolución Democrática (DOF: 28/12/2018), así como los artículos 1, 3, 8 inciso c) e i), 21, 36 y 37 del Reglamento de Afiliación vigente, se informa que los datos recabados por este Partido, serán protegidos en términos de la legislación citada anteriormente.

A este efecto, damos cumplimiento al artículo 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en los siguientes términos:

LA DENOMINACIÓN DEL RESPONSABLE (Frcc. I, Art. 27 LGPDPPSO): Órgano de Afiliación del Partido de la Revolución Democrática.

EL DOMICILIO DEL RESPONSABLE (Frcc. I, Art. 28 LGPDPPSO): Av. Monterrey N° 50, Col. Roma, C.P. 06700, Cuahutémoc México, CDMX.



INICIO | API-Departamento_Juridico.pdf

prd.org.mx/documentos/API-Departamento_Juridico.pdf

AVISO DE PRIVACIDAD

Integral

Este Departamento Jurídico de la Coordinación Nacional del Patrimonio y Recursos Financieros del Partido de la Revolución Democrática, emite el Aviso de Privacidad en su modalidad integral, bajo los siguientes términos:

I. Denominación del responsable.

Departamento Jurídico de la Coordinación Nacional del Patrimonio y Recursos Financieros del Partido de la Revolución Democrática.

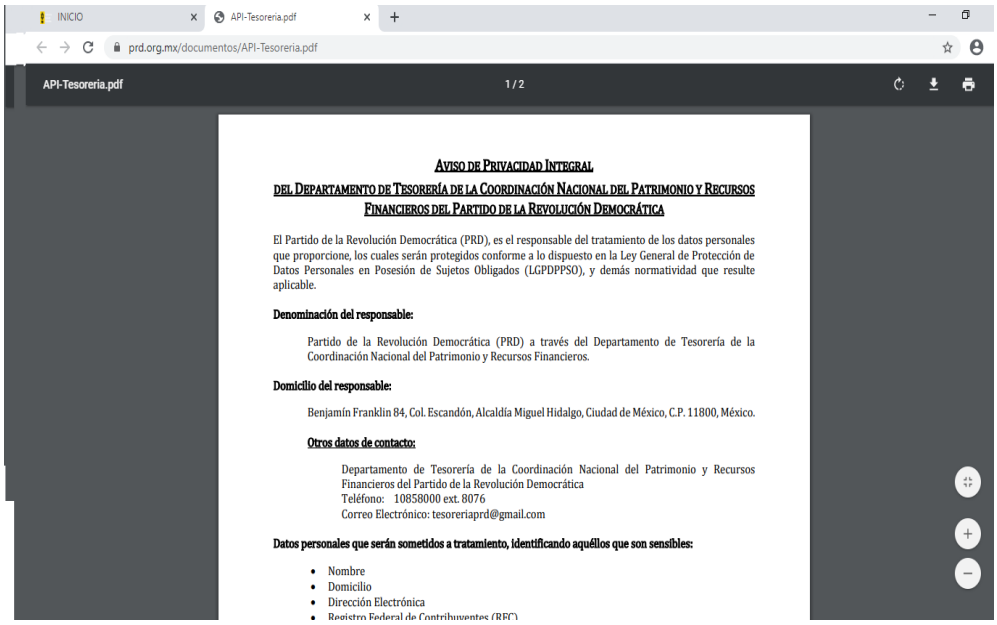
Abreviatura o acrónimo: PRD

II. Domicilio del Responsable.

Benjamín Franklin, número 84, sexto piso, Colonia Escandón, alcaldía Miguel Hidalgo, C.P. 11800, Ciudad de México.

Datos de contacto: juridico_prd_nacional@hotmail.com

III. Datos personales.



INICIO | API-Tesoreria.pdf

prd.org.mx/documentos/API-Tesoreria.pdf

API-Tesoreria.pdf 1 / 2

AVISO DE PRIVACIDAD INTEGRAL

DEL DEPARTAMENTO DE TESORERÍA DE LA COORDINACIÓN NACIONAL DEL PATRIMONIO Y RECURSOS FINANCIEROS DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA

El Partido de la Revolución Democrática (PRD), es el responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y demás normatividad que resulte aplicable.

Denominación del responsable:

Partido de la Revolución Democrática (PRD) a través del Departamento de Tesorería de la Coordinación Nacional del Patrimonio y Recursos Financieros.

Domicilio del responsable:

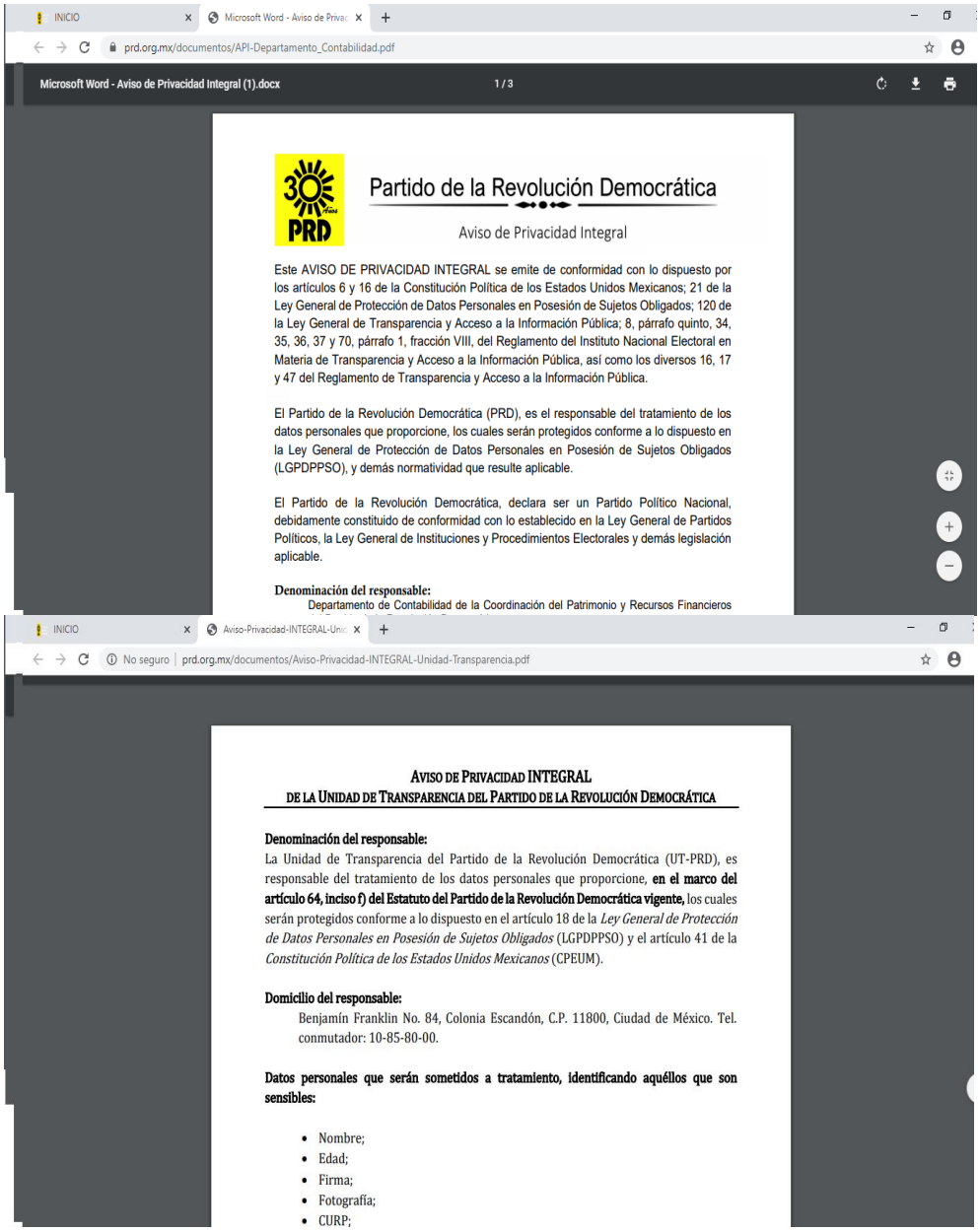
Benjamín Franklin 84, Col. Escandón, Alcaldía Miguel Hidalgo, Ciudad de México, C.P. 11800, México.

Otros datos de contacto:

Departamento de Tesorería de la Coordinación Nacional del Patrimonio y Recursos Financieros del Partido de la Revolución Democrática
Teléfono: 10858000 ext. 8076
Correo Electrónico: tesoreriaprd@gmail.com

Datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles:

- Nombre
- Domicilio
- Dirección Electrónica
- Registro Federal de Contribuyentes (RFC)



Microsoft Word - Aviso de Privacidad Integral (1).docx 1 / 3

prd.org.mx/documentos/API-Departamento_Contabilidad.pdf

Partido de la Revolución Democrática

Aviso de Privacidad Integral

Este AVISO DE PRIVACIDAD INTEGRAL se emite de conformidad con lo dispuesto por los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos; 21 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 120 de la Ley General de Transparencia y Acceso a la Información Pública; 8, párrafo quinto, 34, 35, 36, 37 y 70, párrafo 1, fracción VIII, del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública, así como los diversos 16, 17 y 47 del Reglamento de Transparencia y Acceso a la Información Pública.

El Partido de la Revolución Democrática (PRD), es el responsable del tratamiento de los datos personales que proporcione, los cuales serán protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y demás normatividad que resulte aplicable.

El Partido de la Revolución Democrática, declara ser un Partido Político Nacional, debidamente constituido de conformidad con lo establecido en la Ley General de Partidos Políticos, la Ley General de Instituciones y Procedimientos Electorales y demás legislación aplicable.

Denominación del responsable:
Departamento de Contabilidad de la Coordinación del Patrimonio y Recursos Financieros

No seguro | prd.org.mx/documentos/Aviso-Privacidad-INTEGRAL-Unidad-Transparencia.pdf

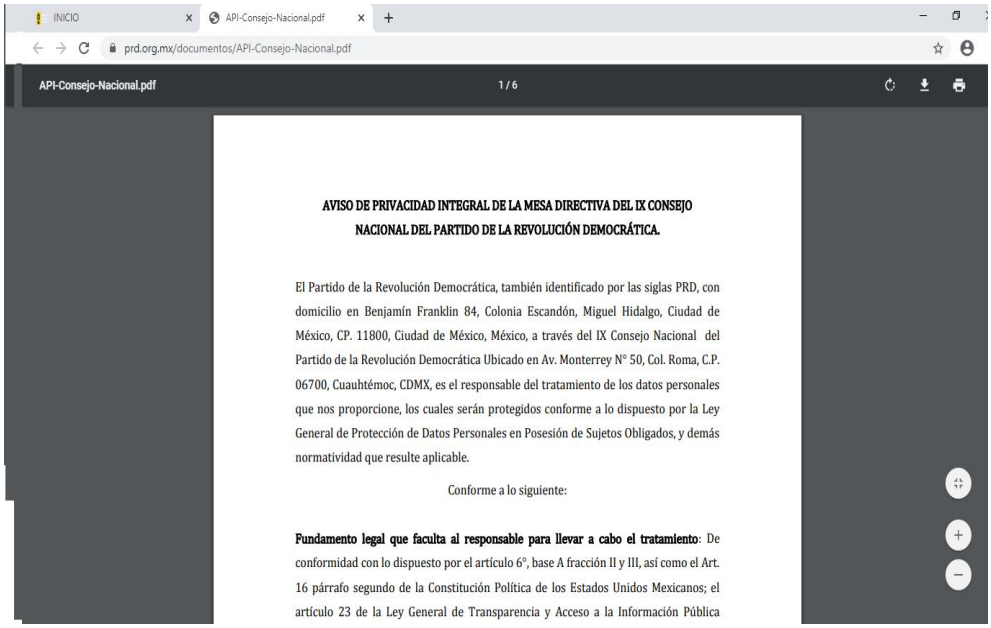
AVISO DE PRIVACIDAD INTEGRAL
DE LA UNIDAD DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA

Denominación del responsable:
La Unidad de Transparencia del Partido de la Revolución Democrática (UT-PRD), es responsable del tratamiento de los datos personales que proporcione, **en el marco del artículo 64, inciso f) del Estatuto del Partido de la Revolución Democrática vigente,** los cuales serán protegidos conforme a lo dispuesto en el artículo 18 de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPPSO) y el artículo 41 de la *Constitución Política de los Estados Unidos Mexicanos* (CPEUM).

Domicilio del responsable:
Benjamín Franklin No. 84, Colonia Escandón, C.P. 11800, Ciudad de México. Tel. conmutador: 10-85-80-00.

Datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles:

- Nombre;
- Edad;
- Firma;
- Fotografía;
- CURP;



INICIO | API-Consejo-Nacional.pdf

prd.org.mx/documentos/API-Consejo-Nacional.pdf

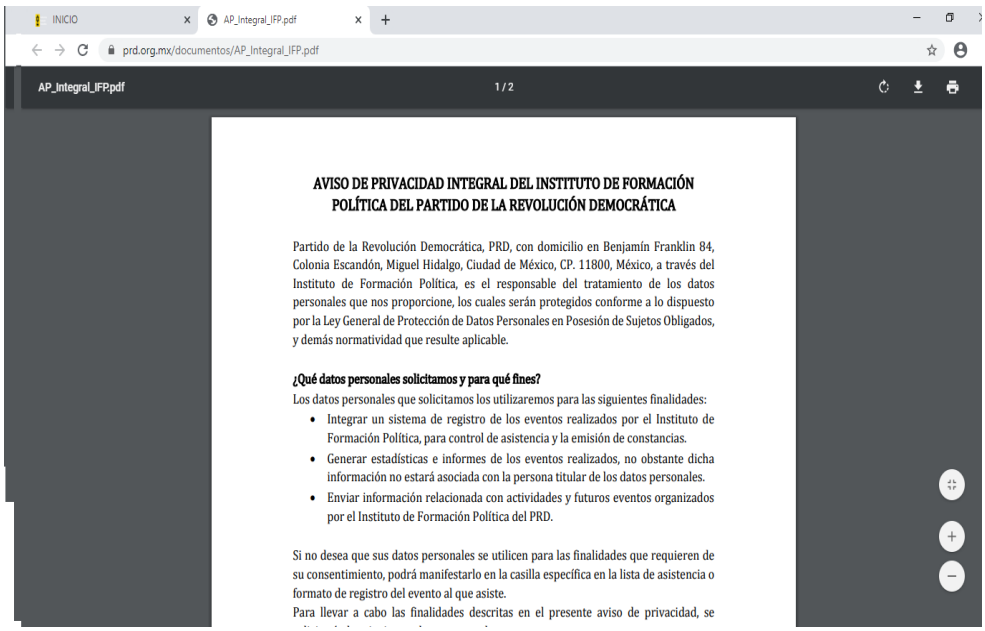
API-Consejo-Nacional.pdf 1 / 6

AVISO DE PRIVACIDAD INTEGRAL DE LA MESA DIRECTIVA DEL IX CONSEJO NACIONAL DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

El Partido de la Revolución Democrática, también identificado por las siglas PRD, con domicilio en Benjamín Franklin 84, Colonia Escandón, Miguel Hidalgo, Ciudad de México, CP. 11800, Ciudad de México, México, a través del IX Consejo Nacional del Partido de la Revolución Democrática Ubicado en Av. Monterrey N° 50, Col. Roma, C.P. 06700, Cuauhtémoc, CDMX, es el responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad que resulte aplicable.

Conforme a lo siguiente:

Fundamento legal que faculta al responsable para llevar a cabo el tratamiento: De conformidad con lo dispuesto por el artículo 6°, base A fracción II y III, así como el Art. 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos; el artículo 23 de la Ley General de Transparencia y Acceso a la Información Pública



INICIO | AP_Integral_IFP.pdf

prd.org.mx/documentos/AP_Integral_IFP.pdf

AP_Integral_IFP.pdf 1 / 2

AVISO DE PRIVACIDAD INTEGRAL DEL INSTITUTO DE FORMACIÓN POLÍTICA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA

Partido de la Revolución Democrática, PRD, con domicilio en Benjamín Franklin 84, Colonia Escandón, Miguel Hidalgo, Ciudad de México, CP. 11800, México, a través del Instituto de Formación Política, es el responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad que resulte aplicable.

¿Qué datos personales solicitamos y para qué fines?

Los datos personales que solicitamos los utilizaremos para las siguientes finalidades:

- Integrar un sistema de registro de los eventos realizados por el Instituto de Formación Política, para control de asistencia y la emisión de constancias.
- Generar estadísticas e informes de los eventos realizados, no obstante dicha información no estará asociada con la persona titular de los datos personales.
- Enviar información relacionada con actividades y futuros eventos organizados por el Instituto de Formación Política del PRD.

Si no desea que sus datos personales se utilicen para las finalidades que requieren de su consentimiento, podrá manifestarlo en la casilla específica en la lista de asistencia o formato de registro del evento al que asiste.

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad, se

Una vez expuesto lo anterior, esta Unidad de Transparencia, procede a puntualizar las siguientes consideraciones de derecho:

- ***CONSIDERACIONES DE DERECHO*** –

La Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A(III), de 10 de diciembre de 1948, refiere en su artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.", a su vez, el artículo 18 de dicho instrumento internacional refiere: "Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia, el artículo 29, punto 2, reza: "En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley, con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática." El punto 3, del artículo 29 dice: "Estos derechos y libertades no podrán en ningún caso ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas." Finalmente: "Nada en la presente Declaración podrá interpretarse en el sentido de que confiere derecho alguno al Estado, a un grupo o a una persona, para emprender y desarrollar actividades o realizar actos tendentes a la supresión de cualquiera de los derechos y libertades proclamados en esta Declaración.

*La Convención Americana sobre Derechos Humanos, suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos, también conocida como Pacto de San José, del 7 al 22 de noviembre de 1969, establece lo siguiente: "**Artículo 1. Obligación de Respetar los Derechos** 1. Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. (...) **Artículo 11. Protección de la Honra y de la Dignidad** (...) 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o a su reputación.*

Dentro del bloque de constitucionalidad, no solo encontramos tratados internacionales que versan específicamente sobre derechos humanos, sino sobre transacciones comerciales o intercambio de datos personales para fines de cooperación internacional entre Estados partes, por ejemplo, el CONVENIO N° 108 DEL CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL Y PROTOCOLO ADICIONAL AL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, A LAS AUTORIDADES DE CONTROL Y A LOS FLUJOS TRASFRONTERIZOS DE DATOS, para cuya comprensión es importante puntualizar lo siguiente:

*"El Foro de Cooperación Económica Asia Pacífico (APEC) aprobó en noviembre de 2004 su Marco de Privacidad, **con el ánimo de fortalecer la protección de la privacidad y permitir los flujos de información[2].** En septiembre de 2007 APEC lanzó igualmente el **"Privacy Pathfinder", que tiene por objeto impulsar la aprobación de normativas[3]** que permitan esclarecer responsabilidades en los flujos internacionales de datos derivados de las*

[2] Énfasis añadido.
[3] *Idem.*

necesidades empresariales, reducir los costes de cumplimiento a la normativa, facilitar a los consumidores instrumentos efectivos de protección de sus derechos, dotar de mayor eficacia a los reguladores y minimizar las cargas administrativas.
[…]

Debe tenerse presente que – con bastante frecuencia – los datos personales de que se trata son de carácter sensible y han sido obtenidos por las autoridades policiales y judiciales como resultado de una investigación referida a personas. ***La voluntad de intercambiar tales datos con las autoridades de otros Estados miembros o adherentes se incrementará si esos Estados dan garantías a la autoridad en cuanto al nivel de protección de los datos. El SEPD (Supervisor Europeo de Protección de Datos)*** [4] *menciona, entre los elementos destacados de la protección de datos, su confidencialidad y seguridad así como las limitaciones de su acceso y su uso posterior. […]*

Ahora bien, el PROTOCOLO ADICIONAL AL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, A LAS AUTORIDADES DE CONTROL Y A LOS FLUJOS TRANSFRONTERIZADOS DE DATOS (Estrasburgo, 8.XI.2001[5]*), refiere lo siguiente:*

Artículo 2.- *Flujos transfronterizados de datos de carácter personal hacia un destinatario que no está sujeto a la jurisdicción de una Parte en el Convenio.*

1. *Cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio* ***sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista.***

Así púes, es posible rastrear, que allende de la voluntad política para proteger los datos personales de las personas, existía una necesidad pujante de asegurar intercambios de información para fines de colaboración internacional para fines diversos, entre ellos, los comerciales.

Otro ejemplo importante es el Tratado Comercial entre México Estados Unidos y Canadá (T-MEC), antes TLCAN, que sin tener un propósito central, ubicado en la protección de datos personales, en efecto, regula ese derecho humano, como se aprecia en la foja 28-6 de la sección intitulada "BUENAS PRÁCTICAS REGULATORIAS" y, que a la letra dice: "Cada Parte procurará poner a disposición del público con prontitud cualquier comentario por escrito que reciba, salvo en la medida de lo necesario para proteger la información confidencial o retener información de identificación personal o contenido inapropiado.". Así, en una amplia gama de tratados internacionales, observamos que pese que en su intitulación no se puntualiza el concepto "protección de datos personales" de hecho, si lo regulan, es esa evolución del derecho protector del habeas data (tener datos), lo que en gran medida ha impulsado al Estado mexicano a colocarse a la altura de las circunstancias ante la comunidad internacional.

El derecho a la protección de datos personales para el sector público, en México, se remonta a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en 2002, particularmente en lo dispuesto por sus artículos 3 Frcc. II y 18 Frcc. II.

El diez de junio de dos mil once, el artículo 1° de la Constitución Política de los Estados Unidos Mexicanos fue reformado para quedar como a continuación se aprecia: "En los

[4] *Idem.*
[5] Apenas un año después de la creación del otrora IFAI.

Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece. Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia. Todas las autoridades, en ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencias, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley […] Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Es importante mencionar que el 24 de junio de 2011 en la Suprema Corte de Justicia, se denunció la posible contradicción de tesis entre los criterios sostenidos por el Primer Tribunal Colegiado en Materia Administrativa y de Trabajo del Décimo Primer Circuito y por el Séptimo Tribunal Colegiado en Materia Civil del Primer Circuito, una vez registrada la contradicción de tesis bajo el número 293/2011, ese máximo tribunal disertó sobre los siguientes temas: a) La posición jerárquica de los tratados internacionales en materia de derechos humanos frente a la Constitución, en ese orden de ideas, "cuando se trate de un conflicto que verse sobre derechos humanos, los tratados o convenciones internacional suscritos por el Estado Mexicano, deben ubicarse propiamente a nivel de la Constitución", de tal posicionamiento derivó la siguiente tesis: "TRATADOS INTERNACIONALES. CUANDO LOS CONFLICTOS SE SUSCITEN EN RELACIÓN CON DERECHOS HUMANOS, DEBEN UBICARSE A NIVEL DE LA CONSTITUCIÓN"; b) El valor de la Jurisprudencia emitida por la Corte Interamericana de Derechos Humanos, al respecto, se determinó que es posible invocar la jurisprudencia de la Corte Interamericana de Derechos Humanos (en adelante CIDH) como criterio orientador cuando se trate de la interpretación y cumplimiento de disposiciones protectoras de derechos humanos. Derivado de tal criterio, surgió la tesis del siguiente rubro: "JURISPRUDENCIA INTERNACIONAL. SU UTILIDAD ORIENTADORA EN MATERIA DE DERECHOS HUMANOS"., además, el Primer Tribunal Colegiado en Materias Administrativa y de Trabajo del Décimo Primer Circuito Señaló en diversas consideraciones que la jurisprudencia internacional en materia de derechos humanos era obligatoria. Con relación al valor de la jurisprudencia emitida por la CIDH, se determinó que ***la jurisprudencia emitida por la Corte Interamericana de Derechos Humanos es vinculante para todos los órganos jurisdiccionales, siempre que dicho precedente favorezca en mayor medida a las personas.***

En otro orden de ideas, las reformas en materia de transparencia, acceso a la información y protección de datos personales contempladas en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicana, (en adelante CPEUM) en dos mil nueve y dos mil catorce, impulsaron la emisión de diversa normatividad con el propósito de garantizar el ejercicio del derecho humano a la protección de datos personales.

Por otra parte, en 2009, se reformó el artículo 16 constitucional el cual establece que toda persona tiene derecho a la protección de sus datos personales, el acceso, rectificación y cancelación de los mismos (derechos ARCO), así como a manifestar su oposición al uso de su información personal, en los términos que fijara la ley. Esta reforma propició la publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010, sin embargo, no sino hasta la reforma constitucional del artículo 6°

de la CPEUM de febrero de 2014, que se fijaron las bases para la promulgación de una Ley General especializada en la protección de datos personales en posesión de los sujetos obligados del sector público, en la cual, evidentemente, están contemplados los partidos políticos, en este caso, el Partido de la Revolución Democrática.

Lo anterior, nos lleva al año dos mil dieciocho, fecha en que se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales de Protección de Datos Personales), en los que se desarrollan y concentran las obligaciones exigibles del derecho a la protección de datos personales en el sector público federal, para evitar la fragmentación o atomización de ordenamientos que puedan repercutir en el cumplimiento efectivo de la LGPDPPSO por parte de los responsables en el sector público.

A partir de la publicación de la LGPDPPSO y de los Lineamientos Generales de Protección de Datos Personales, los partidos políticos, adquirieron la obligación de tratar los datos personales de las personas titulares de dichos datos, en carácter de "sujetos obligados", conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; conducirse mediante los deberes de confidencialidad y seguridad, así como garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), entre otras obligaciones previstas por la LGPDPPSO.

Ahora bien, en atención a que el Partido de la Revolución Democrática, conforme al artículo 41 de la Constitución Política de los Estados Unidos Mexicanos, es: una "entidad de interés público que tiene como finalidad promover la participación del pueblo en la vida democrática, contribuir a la integración de los órganos de representación política y como organizaciones de ciudadanos, hacer posible el acceso de éstos al ejercicio del poder público, de acuerdo con los programas, principios e ideas que postulan y mediante el sufragio universal, libre, secreto y directo, así como las reglas para garantizar la paridad entre los géneros, en candidaturas a legisladores federales y legales", a su vez, esa disposición constitucional establece que: "solo los ciudadanos podrán formar partidos políticos y afiliarse libre e individualmente a ellos; por lo tanto quedan prohibidas la intervención de organizaciones gremiales o con objeto social diferente en la creación de partidos y cualquier forma de afiliación corporativa". Además de lo dispuesto por el artículo 1° de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, este Instituto Político, es un sujeto obligado en materia de protección de datos personales, en el marco del sector público y, por ende, responsable del tratamiento de los datos personales que trata para el ejercicio de sus atribuciones.

Así, entre los "Deberes" previstos en la LGPDPPSO, está el elaborar un documento de seguridad (artículo 35 de la LGPDPPSO) en el cual se describa y de cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen los distintos órganos intrapartidarios de este Partido político. La elaboración de este documento, como instrumento informativo para la sociedad, fue coordinada por la Unidad de Transparencia del Partido de la Revolución Democrática (UT - PRD).

Lo anterior, en virtud de que la UT-PRD, conforme a los artículos 128 a 138 del Estatuto del Partido de la Revolución Democrática vigente al 31 de diciembre de 2019 con relación a la estructura orgánica del PRD y, al ser el órgano intrapartidario especializado en materia

de protección de datos personales, tiene entre otras atribuciones, la de orientar a los órganos intrapartidarios del PRD en el cumplimiento de la LGPDPPSO.

Se precisa que la persona titular de la Unidad de Transparencia, en los términos del Reglamento de Transparencia, Acceso a la Información, Protección de Datos Personales y Gestión Documental del Partido de la Revolución Democrática vigente, preside el Comité de Transparencia del Partido de la Revolución Democrática (CT-PRD), máxima autoridad en materia de protección de datos personales al seno de este Instituto Político, en consonancia con la coadyuvancia del Oficial de Protección de Datos Personales del Partido de la Revolución Democrática.

Ese CT-PRD tiene entre otras funciones, la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización Partido de la Revolución Democrática, de conformidad con las disposiciones previstas en la LGPDPPSO y demás disposiciones que resulten aplicables.

Ahora bien, es importante aludir a la dinámica organizacional, mediante la cual se orquestó la elaboración del Documento de Seguridad consistió en llevar a cabo las siguientes actividades:

-ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD -

A) Se giraron oficios a todos los órganos intrapartidarios establecidos en el Estatuto del Partido de la Revolución Democrática vigente, de los cuales fue posible recabar información útil para la elaboración de este documento;

B) Se concentraron los elementos relacionados al cumplimiento de los requisitos establecidos en la LGPDPPSO.

C) A través de la Unidad y del Comité de Transparencia del Partido de la Revolución Democrática, se realizaron reuniones de trabajo con los órganos intrapartidarios del Partido de la Revolución Democrática, para conocer las medidas de seguridad que deben prevalecer en los sistemas de soporte físico y electrónico, de éstos últimos.

D) Se desarrolló la metodología y un ejemplo de metodología para generar un Sistema de Tratamiento de Datos Personales, mismo que fue notificado a los órganos intrapartidarios de este Instituto político.

E) Se propició una reunión de trabajo con integrantes de los órganos intrapartidarios del Partido de la Revolución Democrática con la finalidad de dar a conocer la metodología para generar este documento y recopilar información adicional de cada uno de ellos.

F) Como consecuencia de dichos acercamientos, se convocó a los órganos intrapartidarios para dar a conocer el borrador del Documento de Seguridad del Partido de la Revolución Democrática.

G) Todas esas actividades, forman parte de un plan trabajo que se desarrolló durante el 2019, en que previa notificación personal, cada órgano intrapartidario fue puesto en conocimiento de los requisitos y metodología para entregar la información sobre los distintos sistemas de tratamiento de datos personales como sigue:

ETAPA 1	***ETAPA 2***	***ETAPA 3***	***ETAPA 4***
Determinación del Inventario de Sistemas de datos personales a considerar en el documento.	*Descripción e Identificación de la estructura de los Sistemas de datos personales.*	*Determinación de las medidas de seguridad y capacitación en materia de protección de datos personales.*	*Integración del documento final ante el Comité de Transparencia del Partido de la Revolución Democrática.*

Así, los distintos órganos intrapartidarios del Partido de la Revolución Democrática que cuentan con sistemas de datos personales, aportaron elementos para requisitar la metodología propuesta, consistentes en información para la integración del Documento de Seguridad del Partido de la Revolución Democrática, con base en los siguientes ejes:

- *Los sistemas de tratamiento de datos personales con que cuentan, su objetivo y el fundamento normativo para llevar a cabo dicho tratamiento.*
- *La descripción e identificación de la estructura de los sistemas de tratamiento de datos personales, mediante la cual se incluyen los datos personales que contienen* ***los sistemas de tratamiento y su idoneidad, la manera en que se obtienen, el administrador del sistema, sus operadores, usuarios, el tipo de soporte en que se encuentran, las características del lugar en que se localizan, si es posible su portabilidad, si existe transferencia y si hay encargados.***
- ***La información de las medidas de seguridad, en donde se incluye la descripción de las existentes, la identificación de riesgos, la determinación de brechas, la elaboración del plan de trabajo, mecanismos de monitoreo y la propuesta de capacitación en medidas de seguridad.***

Con la información que fue remitida por los órganos intrapartidarios del PRD, se integra un instrumento informativa que se enmarca en el rubro de transparencia proactiva, que da cuenta del estado actual del Documento de Seguridad del Partido de la Revolución Democrática.

Es oportuno considerar que, en caso de ser necesario, de conformidad con el artículo 89,

fracciones XII y XIII de la LGPDPPSO, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) está facultado para proporcionar apoyo técnico a los responsables, para el cumplimiento de las obligaciones establecidas en dicha Ley, así como para divulgar y emitir las recomendaciones, estándares y mejores prácticas en las materias reguladas por la misma

Marco normativo:

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- *La protección de datos personales puede rastrearse desde la Declaración Universal de Derechos Humanos, cuyas disposiciones aplicables fueron citadas previamente, para prevenir que, en el futuro, se volviera, entre otros motivos, a vulnerar los datos personales y la privacidad de las personas para fines ilegítimos o criminales, tal como ocurrió con el tratamiento sistematizado, relevante y masivo de las personas judías para ser identificadas y capturadas. Posteriormente, el espíritu de esas disposiciones, fue retomado, entre otros instrumentos internacionales, en la confección de la Declaración Americana de Derechos Humanos.*

- *Artículos 1°, 6° y el segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos;*

- *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017;*

- *Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero 2018;*

- *Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018;*

- *Estatuto del Partido de la Revolución Democrática (vigente del 2018 y del 2019);*

- *Declaración de Principios del Partido de la Revolución Democrática (vigente);*

- *Programa de Acción del Partido de la Revolución Democrática (vigente);*

- *Reglamento del Congreso Nacional del Partido de la Revolución Democrática (vigente);*

- *Reglamento de las Coordinadoras de Autoridades Locales del Partido de la Revolución Democrática (vigente);*

- *Reglamento de Transparencia, Acceso a la Información, Protección de Datos Personales y*

Gestión Documental del Partido de la Revolución Democrática (vigente);

- *Reglamento de Disciplina Interna del Partido de la Revolución Democrática del Partido de la Revolución Democrática (vigente);*
- *Reglamento de Afiliación del Partido de la Revolución Democrática (vigente);*
- *Reglamento de los Consejos del Partido de la Revolución Democrática (vigente);*
- *Reglamento de las Direcciones del Partido de la Revolución Democrática (vigente);*
- *Reglamento de Elecciones del Partido de la Revolución Democrática (vigente);*
- *Reglamento de las Direcciones de Comunicación Nacional y Estatales del Partido de la Revolución Democrática (vigente);*
- *Reglamento del Instituto de Formación Política del Partido de la Revolución Democrática (vigente);*
- *Reglamento de la Organización Nacional de Mujeres del Partido de la Revolución Democrática (vigente);*
- *Reglamento del Órgano de Justicia Intrapartidaria del Partido de la Revolución Democrática (vigente);*
- *Reglamento del Patrimonio y Recursos Financieros (vigente);*
- *Reglamento de la Organización Nacional de las Juventudes de Izquierda del Partido de la Revolución Democrática (vigente).*
- *Reglamento de las Direcciones de Comunicación Nacional y Estatales (vigente);*

Ámbito de aplicación y observaciones generales.

En atención a los deberes a que se refiere la LGPDPPSO (de confidencialidad y de seguridad) el presente documento, es aplicable para todos los órganos intrapartidarios del Partido de la Revolución Democrática (PRD) que, en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ***ya sea que administren sistemas completos, o el tramo de información que le corresponda, sin importar si recaban datos personales de manera directa o indirecta de las personas titulares de datos personales.***

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma

numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato.

Todos los servidores partidistas que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando con su eliminación. Cabe mencionar que, la obligación de confidencialidad, debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales sea porque hayan cambiado de funciones o cuando la relación organizacional con el Partido de la Revolución Democrática haya concluido.

Además de las funciones y obligaciones de los servidores partidistas involucrados en los distintos tratamientos de datos personales al seno de este Instituto político, establecidas de manera específica en el análisis de cada uno de los Sistemas, de manera general, deberán de observarse las siguientes:

Funciones genéricas de los servidores partidistas del Partido de la Revolución Democrática en cualquier nivel de tratamiento.

- *Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin;*
- *Estar capacitada o capacitado en materia de tratamiento de datos personales;*
- *Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales;*
- *Cumplir a cabalidad con los roles de: Responsable; Administrador; u Operador del Sistema; o bien como Enlace de datos personales.*

De manera particular y de conformidad con los cargos, encargos y/o designaciones de los servidores partidistas, se definen cuatro roles básicos en el tratamiento de los datos personales:

Sus funciones son las siguientes:

- ***Responsable del Sistema:** Sin menoscabo de los descargos de responsabilidades que se diseñen mediante mecanismos administrativos, será la persona titular o los integrantes del órgano intrapartidario donde se administre el Sistema de que se trate. Deberá:*

1. *Dar aviso a la Unidad de Transparencia y al Departamento Jurídico de la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática, que también funge como Oficialía de Protección de Datos Personales del Partido de la Revolución Democrática, de los Sistemas que involucren tratamiento de datos personales, a cargo de dicha Unidad Administrativa;*

2. *Designar a la persona administradora del Sistema; y*
3. *Validar que la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.*

- ***Persona administradora del Sistema:*** *Será la persona servidora partidista a quien designe de manera expresa la persona titular o las personas integrantes del órgano intrapartidario competente y tenga a su cargo la responsabilidad de la administración del sistema y de los operadores, por lo cual deberá:*

1. *Mantener actualizado el Sistema;*
2. *Designar a las personas servidoras partidistas que deban tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos;*
3. *Autorizar los accesos de las personas servidoras partidistas, determinar los privilegios y limitantes correspondientes, así como llevar un registro de los mismos*
4. *Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.*

- ***Operador (as, es)***

1. *Sus funciones quedan determinadas de acuerdo al perfil que se haya asignado en el tratamiento de los datos personales de cada uno de los sistemas.*

- ***Enlace de datos personales***[6]

1. *Conocer del Inventario de Sistemas que involucren tratamiento de datos personales y por cada uno, conocer el tipo de datos personales que se recaban y el nombre del Encargado por cada Sistema.*
2. *Dar seguimiento a las acciones de capacitación para tos servidores partidos involucrados en el tratamiento de los datos personales.*
3. *Atender a los requerimientos de información que solicite la Unidad de Transparencia, el Departamento Jurídico de la Coordinación de Patrimonio y Recursos Financieros de la Coordinación de Patrimonio y Recursos Financieros, o el Órgano de Justicia Intrapartidaria del Partido de la Revolución Democrática.*

El incumplimiento a lo establecido en el Documento de Seguridad, así como a lo establecido por la LGPDPPSO y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, causará la aplicación de medidas de apremio y/o de sanciones, que se detallan en los documentos básicos y reglamentos vigentes del Partido de la Revolución Democrática.

En caso de existir figura de "Encargado", en la formalización de la prestación de algún servicio que implique la transferencia de datos para su tratamiento, deberá atenderse a lo previsto en el artículo 59 de la LGPDPPSO y los artículos correspondientes de los

[6] Corresponde a la figura del Enlace de Transparencia.

Lineamientos Generales ***de Protección de Datos Personales para el Sector Público (LGPDPPSO), que se refieren a la existencia de algún instrumento jurídico que incluya cláusulas sobre el tratamiento de datos personales conforme a las instrucciones del responsable (el PRD), que prevean que los datos no se tratarán para finalidades distintas a las previstas, que establezcan que se implementarán medidas de seguridad, que se informará al responsable en caso de vulneración, que se guardará confidencialidad respecto de los datos personales, que éstos se suprimirán o devolverán al concluir la relación jurídica en atención a las normas jurídicas sobre su conservación y que se abstendrán de transferirlos salvo determinación del responsable en atención a la normatividad y de conformidad con el aviso de privacidad correspondiente.***

Desarrollo

1. ***Inventario de Sistemas de Tratamiento de Datos Personales***

Los sistemas que se detallan en el presente documento *son aquellos que contienen datos personales, que se encuentran tanto en soporte electrónico como físico.*

Se presentan por órgano intrapartidario y en orden de mención con base en el los documentos básicos y reglamentos del Partido de la Revolución Democrática, a saber:

a) Dirección Nacional Extraordinaria del Partido de la Revolución Democrática;

b) Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática del Partido de la Revolución Democrática;

c) Coordinación de la Organización Nacional de Mujeres, del Partido de la Revolución Democrática (nacional);

d) Órgano de Justicia Intraprtidaria del Partido de la Revolución Democrática;

e) Órgano de Afiliación del Partido de la Revolución Democrática;

f) Órgano Técnico Electoral del Partido de la Revolución Democrática;

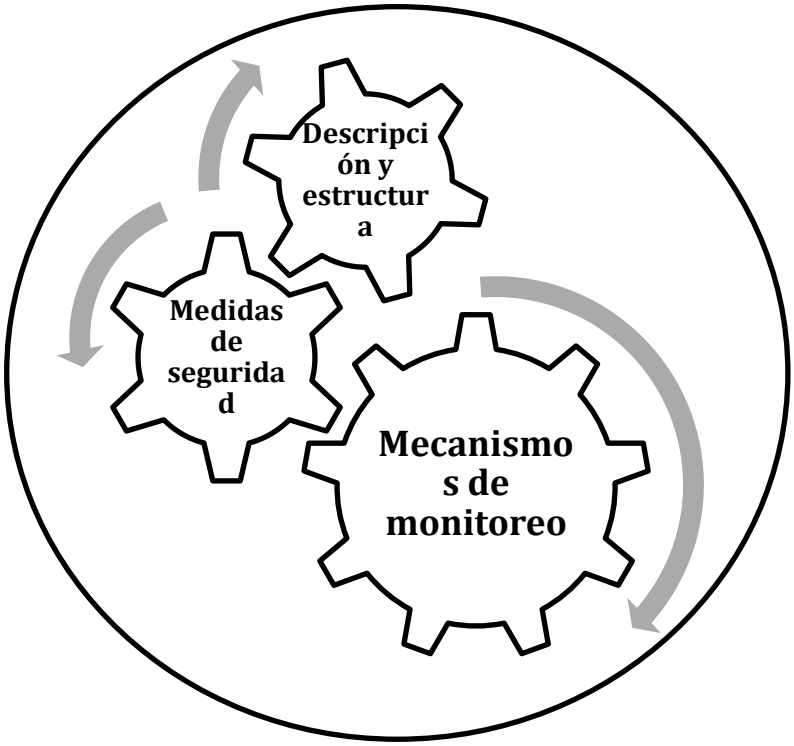
g) IX Consejo Nacional del Partido de la Revolución Democrática;

h) Representación del Partido de la Revolución Democrática ante el Consejo General del Instituto Nacional Electoral; y

i) Representación del Partido de la Revolución Democrática ante el Registro Federal de Electores del Instituto Nacional Electoral.

En los siguientes apartados, partiendo de la información que cada órgano intrapartidario brindó en su momento, se abordará cada uno de los Sistemas señalando su descripción, estructura y medidas de seguridad. Posteriormente, se abordarán análisis de riesgos; de brecha; y el plan de trabajo.

SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES



1- Descripción y estructura de los sistemas de tratamiento de datos personales

En la descripción de cada sistema de tratamiento de datos personales, dependiendo de los insumos que hayan sido aportados por cada órgano intrapartidario, se señala el objetivo, fundamento legal, servidor partidista que administra el sistema, operador (a, es) y, usuarios del mismo y tipo de datos personales que se tratan el Sistema, ***entre otras*** *cuestiones. La descripción general se lleva a cabo conforme a los siguientes indicadores:*

1.	*Objetivo*	*Propósito/fin para el que fue diseñado, desarrollado, construido o pensado el Sistema*
2.	*Fundamento legal*	*Disposición legal, en donde se mencione la obligatoriedad de contar con el sistema en cuestión y/o la atribución de recabar en atención a sus facultades*
3.	*Tipo de dato*	*Lista de datos personales que contiene el sistema*

	personal	*y su idoneidad.*
4.	*Forma de obtención de los datos personales*	*Puede ser directa o indirecta. La directa es aquella que se recaba directamente del titular de los datos personales y la indirecta se refiere a aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular.*
		Algún otro sistema.
5.	*Administrador del sistema*	*Nombre y cargo de servidor público que opera el sistema o sistemas, del órgano intrapartidario en cuestión del PRD.*
6.	*Operadores*	*Nombre y cargo del servidor partidista que opera el sistema de datos personales en cuestión.*
7.	*Usuarios*	*Ciudadano, servidor partidista o alguna otra figura que hace uso del sistema.*
8.	*Tipo de soporte*	*Puede ser físico, electrónico o combinado.*
9.	*Características del lugar donde se resguardan*	*Inmueble, piso, cuadrante, oficina, PC, etc.*
10.	*Portabilidad de datos personales.*	*Derecho que tiene el titular de los datos a obtener una copia de sus datos personales, cuando se encuentren en un formato estructurado y comúnmente utilizado, o a solicitar su transmisión a un responsable receptor, cuando es técnicamente posible, el titular hubiera facilitado directamente sus datos al responsable transmisor y el tratamiento de estos se base en su consentimiento o en la suscripción de un contrato.*
11.	*Transferencia de datos personales*	*Prestador de servicios – persona física o moral, pública o privada, ajena al PRD-, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de la Secretaría y si se cuenta con subcontratación de servicios. Adicionalmente, señalar si se cuenta con proveedor de servicios de cómputo en la nube y otras materias.*
12.	*Encargado.*	*Prestador de servicios -persona física o moral, pública o privada, ajena a la SFP-, que solo o*

conjuntamente con otros, trate datos personales a nombre y por cuenta de la Secretaría y si se cuenta con subcontratación de servicios Adicionalmente señalar si se cuenta con proveedor de servicios de cómputo en la nube y otras materias."

Acto seguido, la Unidad de Transparencia, procedió a verter las manifestaciones que los órganos intrapartidarios del Partido de la Revolución Democrática, con relación a la descripción de los distintos "sistemas de protección de datos personales".

"2- Medidas de Seguridad

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permitan proteger los datos personales.

De manera particular, el artículo 31 dispone que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confiabilidad, integridad y disponibilidad.

A su vez, el artículo 33 prevé que para establecer y mantener las medidas de seguridad para la protección de los datos personales, el sujeto obligado deberá realizar las siguientes actividades:

- *Crear políticas internas para la gestión y tratamiento de los datos personales que consideren su obtención, uso y posterior supresión.*
- *Definir funciones y obligaciones del personal involucrado en el tratamiento de datos personales.*
- *Elaborar un inventario de los datos personales y de los sistemas de tratamiento.*
- *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las*

faltantes en la organización del sujeto obligado.

- *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas de seguridad implementadas, así como las amenazas y vulneraciones.*

- *Monitorear las medidas de seguridad implementadas, así como las amenazas y vulneraciones.*

- *Diseñar y aplicar distintos niveles de capacitación del personal, dependiendo de sus roles y responsabilidades en el tratamiento de datos personales.*

Derivado de lo anterior, el Documento de Seguridad debe contener al menos el: a) Inventario de datos personales y de los sistemas de tratamiento; b) las funciones y obligaciones de las personas que tratan datos personales; c) el análisis de riesgo; d) el análisis de brecha; e) los mecanismos de monitoreo y revisión de las medidas de seguridad; y el programa general de capacitación.

En este sentido, en el presente apartado se integra la información que los distintos órganos intrapartidarios del Partido de la Revolución Democrática describieron como la determinación de las medidas de seguridad de cada uno de los sistemas de tratamiento de datos personales con que cuenta la dependencia y que entregaron durante la Etapa 3 del Plan de Trabajo referido en la introducción bajo los siguientes conceptos:

1. Medidas de seguridad.

Las medidas de seguridad se abordarán en tres modalidades: administrativas, físicas y técnicas.

***Las medidas de seguridad administrativas** se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación clasificación y borrado seguro de la información, así como la sensibilización y capacitación de los servidores partidistas, en materia de protección de datos personales.*

*Por su parte, **las medidas de seguridad físicas,** son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.*

*Finalmente, **las medidas de seguridad técnicas,** son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.*

Como medidas de seguridad, de manera general, en el Partido de la Revolución Democrática, se cuenta con las siguientes:

- ***De tipo administrativo:***

o *La Dirección Nacional Extraordinaria, a través de la Coordinación de Patrimonio y Recursos Financieros del PRD, en el ámbito nacional, así como otros órganos intrapartidarios del PRD, salvaguarda la integridad y seguridad de las personas, bienes, activos e instalaciones del PRD, mediante procedimientos y mecanismos institucionales de identificación y prevención de riesgos de seguridad, como son: Designar por oficio a las personas enlaces de transparencia y protección de datos personales, así como a cualquier otro servidor partidista adscrito a las áreas u órganos de este Partido que tenga por función permanente o temporal tratar datos personales en el marco de alguna de sus líneas de acción.*

- ***De tipo físico:***

o *La Dirección Nacional Extraordinaria, a través de la Coordinación de Patrimonio y Recursos Financieros del PRD, en el ámbito nacional, así como otros órganos intrapartidarios del PRD, salvaguarda la integridad y seguridad de las personas, bienes, activos e instalaciones del PRD, mediante procedimientos y mecanismos institucionales de identificación y prevención de riesgos de seguridad, como son:*

a) Prevenir el acceso no autorizado al perímetro de la organización del PRD, sus instalaciones físicas, áreas críticas, recursos e información, a través de un registro de visitantes, salvo que se trate de personas que soliciten ejercer su derecho de acceso a la información, pues en ese caso, se les invita a acudir directamente a la Unidad de Transparencia que está en la Planta Baja, sin poder acceder a ninguna otra zona del edificio sede de la Dirección Nacional Extraordinaria del Partido de la Revolución Democrática.

b) Se cuenta con normas, procedimientos y medidas de seguridad contemplados en el Programa Interno de Protección Civil que contienen el diseño y establecimiento de lineamientos de

salvaguarda aplicables al interior de los inmuebles, considerando sus características y el tipo de actividad o servicio prestado, con el propósito de reducir al mínimo la incidencia de riesgos como: 1) incendios; 2) inundaciones; 3) terremotos; entre otros posibles escenarios.

c) Proteger los recursos móviles y portátiles y cualquier soporte físico o electrónico que pueda salir del Partido de la Revolución Democrática.

En el Partido de la Revolución Democrática se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles de entrada y salida, como son: control en el uso de aparatos eléctricos y electrónicos; control en el ingreso y egreso de aparatos, equipos, mobiliario, documentos y materiales mediante pase de salida autorizado por un responsable del Área especializada.

d) Proveer los equipos que contienen almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Los equipos de cómputo de escritorio y portátiles que la CPRF-PRD, asigna a los servidores partidistas y órganos intrapartidarios correspondientes para el cumplimiento de sus funciones, así como los equipos destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los Sistemas de información institucionales, cuentan con un programa de mantenimiento periódico en el que se ejecutan acciones preventivas y, en su caso, correctivas respaldadas con personal especializado, con el que se promueve un mantenimiento eficaz, disponibilidad de equipos y la información que hospedan.

Asegurar que se realicen respaldos periódicos de la información relacionada con las funciones institucionales que lleva a cargo y mantener la información, en términos de lo dispuesto por las disposiciones jurídicas vigentes, durante el periodo que tenga el resguardo de éste.

- *El Instituto de Formación Política del Partido de la Revolución Democrática, a través de la Coordinación de Patrimonio y Recursos Financieros del PRD, con relación a las medidas de seguridad físicas, que se practican en este Instituto político, refirió lo siguiente: Son un "conjunto de acciones y mecanismo para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativo más no limitativa, se debe considerar las siguientes actividades: Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; Prevenir el daño o interferencia a la instalaciones físicas, áreas críticas de la organización, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico e electrónico, que pueda salir fuera de las instalaciones de la organización; y proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad funcionalidad e integridad.*

De tipo Técnico:

Se consideran aquellas medidas de seguridad aplicables para los sistemas de tratamiento de datos en soporte electrónico que alberga la DNE, a través de la CPRF, hardware y software.

a) Para prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.

El acceso a las bases de datos de ambientes productivos es exclusivo para personal adscrito a la CPRF y los órganos intrapartidarios. El acceso a las bases de datos se efectúa a través de asignación de contraseñas para ese fin y al cual no tiene acceso la generalidad de los usuarios de los equipos y correos electrónicos.

b) Para generar un esquema de privilegios con la finalidad de que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

Las funciones del usuario de los sistemas de información institucionales son definidas por las áreas responsables de los procesos respectivos, quienes son también los responsables de los procesos respectivos, quienes son también los responsables de validar que tal perfil de usuario se apegue a los requerimientos funcionales.

c) Para revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento, en su caso de software y hardware que pudiera adquirirse.

Como parte de los servicios de seguridad informática, se dispone de la ejecución de pruebas de vulnerabilidad bajo demanda, con frecuencia variable por semestre, los cuales se aplican a sistemas de información productivos o próximos a liberarse u de cuyo resultado se entregan reportes que describen los elementos de configuración o la plataforma tecnológica que resultan susceptibles de explotación de amenazas conocidas, las cuales se usan para mejorar las condiciones de seguridad de la información y el sistema asociado.

Además, se realiza una validación del éxito de los respaldos realizado y en caso de que estos no fueran exitosos, personal de la Coordinación de Patrimonio y Recursos Financieros propicia la elaboración manual del respaldo. En caso de reincidencia en la falla de los respaldos, personal de la CPRF, levanta un incidente a grupos de soporte para que tomen las acciones colectivas necesarias.

d) Para gestionar las comunicaciones, operativas y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

La CPRF, lleva a cabo un monitoreo diario de portales, mediante el cual se identifican aquellos portales o sistemas de información que están fuera de servicio, el monitoreo se realiza tres veces al día y se complementa con las alertas que arroja el sistema de monitoreo del centro de datos.

Los sistemas de información institucionales, operan desde centros de datos resguardados físicamente con personal de seguridad. El centro de datos resguardados físicamente por servidores partidistas designados para tal efecto. El centro de datos, se protege mediante la aplicación de un protocolo antiincendios, control de acceso físico, respaldo de suministro eléctrico, todos ellos monitoreados constantemente, lo cual es complementado con una inspección física diaria.

De manera general, la seguridad lógica de los sistemas de información es resguardada, a través de la verificación de la calidad de los productos y servicios que se adquieren para garantizar ese propósito:

Por lo anterior, estas medidas ya no serán abordadas en el análisis de las medidas de seguridad específicas por cada uno de los Sistemas, salvo que se cuente adicionalmente con medidas de seguridad físicas y/o técnicas especiales en alguno de los mismos reportadas por las distintas unidades administrativas.

En el caso de los sistemas en soporte electrónico administrados por un Encargado, se atiende a las medidas de seguridad establecidas en el instrumento jurídico que se haya formalizado y que deben ser equivalentes con las previstas en el Documento de Seguridad para cada sistema de tratamiento.

Para conocer la información provista al respecto por otros órganos intrapartidarios, se remite a la persona lectora a la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, que puede consultarse mediante el siguiente hipervínculo: https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2019/10S_Ordinaria_29-10-2019.pdf

Análisis de riesgos.

En el establecimiento de las medidas de seguridad, se deben considerar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cualitativo, sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad, tanto en la información de los datos personales como en los recursos involucrados. Este apartado se desarrolló tomando en cuenta:

1) *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de sectores afines a los Partidos políticos;*

2) *El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*

3) *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*

4) Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;

5) La sensibilidad de los datos personales tratados;

6) El desarrollo tecnológico;

7) Las posibles consecuencias de una vulneración para los titulares;

8) El número de titulares;

9) Las posibles vulneraciones;

10) Las transferencias, en su caso.

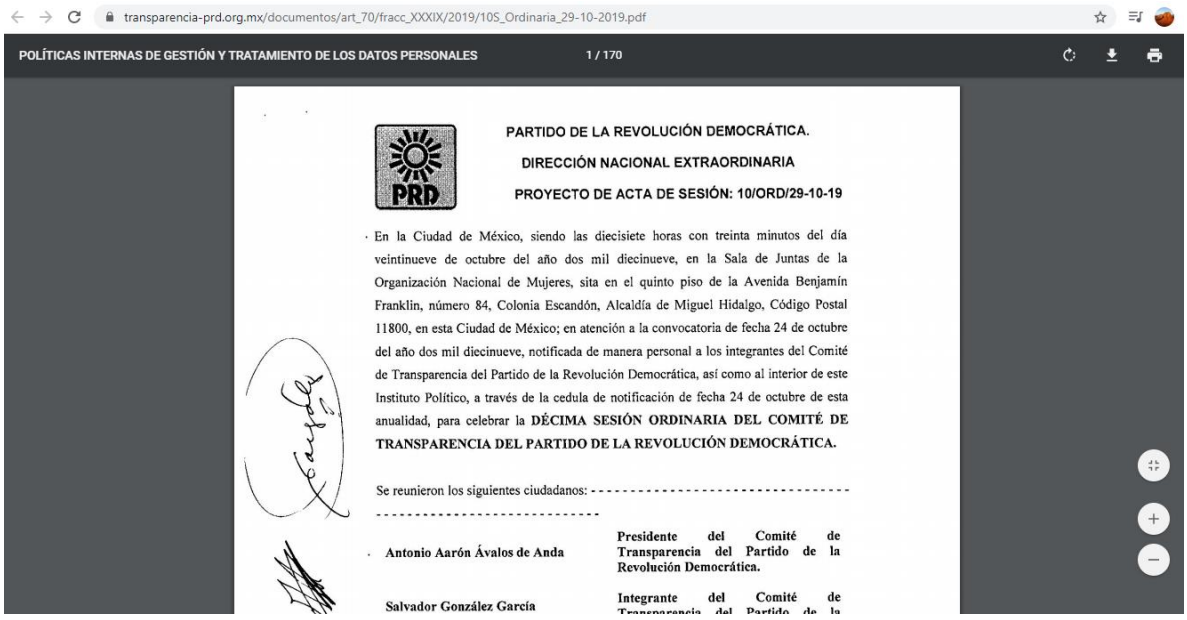
FACTOR	***DESCRIPCIÓN***
Personas	*Servidor partidista que se encuentra relacionado con la ejecución del sistema de forma directa o indirecta.*
Procesos	*Conjunto interrelacionado entre sí, de actividades y tareas necesarias para llevar a cabo en el tratamiento de datos personales.*
Tecnología	*Conjunto de herramientas tecnologías que intervienen de manera directa o indirecta en el Sistema.*
Infraestructura	*Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el sistema de datos.*

CLASIFICACIÓN	***SITUACIONES A RESOLVER***
TICs	*Tecnologías de la información y Comunicación (hardware y software).*
Capacitación	*Desconocimiento de los procesos*
Control	*Falta de control.*
Recursos	*financieros, materiales.*
Factor	*Humano.*

TIPO DE	***DESCRIPCIÓN***

CONTROL	
Interno	*Depende del área u órgano intrapartidario (Departamento de Recursos Humanos e Informática de la CPRF del PRD)*
Externo	*Depende de otro órgano intrapartidario del PRD (esto se actualiza con cualquier otra área distinta al DRHI de la CPRF del PRD).*
Terceros	*En caso de que se requiera de entes externos al Partido de la Revolución Democrática.*

Ahora bien, los órganos intrapartidarios del PRD, en distintos nivel de cumplimiento, se pronunciaron con relación a las medidas de seguridad físicas y administrativas lo cual puede apreciarse en sus manifestaciones en la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, que puede consultarse mediante el siguiente hipervínculo: https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2019/10S_Ordinaria_29-10-2019.pdf, ***que por obvio de repeticiones, se tiene por reproducida en el presente:***


transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2019/10S_Ordinaria_29-10-2019.pdf

POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES 1 / 170

PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

DIRECCIÓN NACIONAL EXTRAORDINARIA

PROYECTO DE ACTA DE SESIÓN: 10/ORD/29-10-19

En la Ciudad de México, siendo las diecisiete horas con treinta minutos del día veintinueve de octubre del año dos mil diecinueve, en la Sala de Juntas de la Organización Nacional de Mujeres, sita en el quinto piso de la Avenida Benjamín Franklin, número 84, Colonia Escandón, Alcaldía de Miguel Hidalgo, Código Postal 11800, en esta Ciudad de México; en atención a la convocatoria de fecha 24 de octubre del año dos mil diecinueve, notificada de manera personal a los integrantes del Comité de Transparencia del Partido de la Revolución Democrática, así como al interior de este Instituto Político, a través de la cedula de notificación de fecha 24 de octubre de esta anualidad, para celebrar la **DÉCIMA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.**

Se reunieron los siguientes ciudadanos: ----------

Antonio Aarón Ávalos de Anda — Presidente del Comité de Transparencia del Partido de la Revolución Democrática.

Salvador González García — Integrante del Comité de

No obstante, el Departamento de Recursos Humanos e Informática de la Coordinación de Patrimonio y Recursos Financieros de la Coordinación de Patrimonio y Recursos Financieros del PRD, es un área facultada para dar soporte técnico a todo el Partido en cuanto hace a medidas de seguridad técnicas. En esa inteligencia, se procede a describir las manifestaciones de dicho Departamento:

Mediante oficio CPRF-DRHI-0011-2019, el DRHI de la CPRF del PRD, realizó manifestaciones coincidentes con otros órganos intrapartidarios y, en lo particular, refirió que que los requerimientos regulatorios, códigos de conducta o mejores prácticas para un

sector específico, en este caso, los partidos políticos, se ajustan a los consagrados en la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, Normas Mexicanas y Normas Oficiales Mexicanas, tesis, tesis aisladas y jurisprudenciales que guardan relación con la materia, lineamientos, acuerdos y guías que emite el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Además, se refirió al valor de los datos personales, como considerable, pues estimó que su riesgo era "MEDIO", agrupándose de la siguiente forma:

a) ***Identificativos:*** *Nombre completo, domicilio, fecha de nacimiento, edad, número telefónico, estado civil, lugar de nacimiento, nacionalidad, sexo, fotografía, registro federal de contribuyentes, clave única de Registro de Población y firma;*

b) ***Datos electrónicos:*** *Correo electrónico;*

c) ***Datos académicos:*** *Títulos, certificados, reconocimientos, constancias, diplomas, cédulas profesional;*

d) ***Datos laborales:*** *Aspiraciones laborales, documentos de reclutamiento y selección, estudios realizados, nombres de las escuelas, periodo, número de años cursados, comprobantes, nombramientos, referencias laborales, número de seguro social, experiencia laboral, referencias personales, datos familiares;*

e) ***Datos Patrimoniales:*** *Créditos hipotecarios, número de cuenta bancaria, beneficiario de la cuenta bancaria, información fiscal, descuentos por orden.*

El Departamento de Recursos Humanos e Informática de la Coordinación Nacional de Patrimonio y Recursos Financieros, a continuación, refirió:

"De acuerdo con la información contenida en el "Estudio sobre el valor económico de los datos personales", elaborado por la Asociación Mexicana de Internet A.C. (AMPICI), ahora Asociación de Internet.mx y la Secretaría de Economía, en una encuesta realizada donde el valor de 0 a 10, se aprecian cifras que muestran el análisis comparativo de los principales tipos de datos ya sean sensibles o no sensibles, a los cuales, los individuos participantes les asignaron una mayor importancia como resultado se la pregunta `... en una escala de 0 a 10, para cada uno de los siguientes datos… califique el nivel de importancia para usted preservar/cuidar.´

Se retoman dichos resultados en un intento de mostrar el valor que pudiese otorgarse a los datos personales recabados por este Departamento, destacando que el promedio de los datos no sensibles, donde se incluyeron los datos financieros y patrimoniales, es de 7.5, en una escala de valoración de 0 a 10, siendo superior al promedio de los datos sensibles del orden de 6.6.

Es importante destacar que los datos financieros y patrimoniales, son los datos a los cuales los individuos participantes, les asignaron una mayor importancia con una calificación de 8.7, seguido de los datos biométricos con el 8.1 y, los datos legales con una evaluación de 7.8.

En los datos de identificación y contacto se obtuvo un promedio de 7.8, donde la firma electrónica es el dato calificado más valioso con 9.2, seguido de la firma autógrafa 9.1 y los datos de domicilio 9.1. Le siguen en importancia los números telefónicos, tanto el teléfono particular como el número del teléfono celular. Los datos de identificación más comunes como edad, nacionalidad y estado civil, son los considerados de menor importancia.

En lo referente a los datos laborales, se obtuvo una calificación promedio de 7.4, observándose una mayor calificación a los datos e información generada durante los procesos de reclutamiento, selección y contratación con 7.9.

Los datos académicos se observó una calificación promedio de 7.6. Los individuos participantes de mayor importancia el dato (número de folio) de la cédula profesional con 8.4 de calificación, seguida de los títulos y certificados con una calificación de 7.7-

Los datos financieros o patrimoniales son los que significaron una mayor importancia para los individuos participantes con una calificación promedio de 8.7. Se destacan por su importancia los datos relacionados con información adicional de la tarjeta, por ejemplo, fecha de vencimiento, código de seguridad, datos de la banda magnética y PIN, con una calificación de 9.2 y de los números de tarjetas de crédito con 9.1.

"Las gráficas con los resultados expuestos se encuentran disponibles en https://clustertic.org/wp-content/uploads/2016/valor_eco_Datospersonales_FINAL.pdf

Su ciclo de vida depende en gran medida de los efectos para los cuales sea necesario su uso; esto es, hay datos que por la naturaleza del Departamento de Recursos Humanos se utilizan constantemente para realizar el pago de los salarios, otros donde su ciclo de vida depende de su periodo de vigencia, (por ejemplo, la credencial de elector), la cual es necesario renovar para que esta surta los efectos de identificación y/o votar. Hay algunos otros datos cuyo ciclo de vida pareciera inalterable, pero en este Departamento cobran gran importancia, tal y como lo es un cambio de reincidencia, donde el domicilio del trabajador fue aportado al momento del ingreso y es el que quedó registrado ante el IMSS y es necesario realizar el cambio previniendo cualquier aclaración. El ciclo de vida de los datos personales utilizados en el Departamento de Recursos Humanos es el que se presenta a continuación:

DATO	CAPTURA DE DATOS Cómo se capturan y/o de donde se obtienen los datos	CLASIFICACION/ALMACENAMIENTO Como se clasifican o almacenan y donde se conservan	USO/TRATAMIENTO El uso o tratamiento que se d[illegible]a los datos (fi[illegible]dad)	CESION O TRANSFERENCIA DE LOS DATOS A UN TERCERO PARA SU TRATAMIENTO Las posibles cesiones o transferencias de los[illegible]os a tercero/s	DESTRUCCION El plazo de conservación y el modo de destruirlos
Nombre completo	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para identificar a los trabajadores del Partido Político	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público Instituto Nacional Electoral (INE) Autoridades jurisdiccionales estatales o federales Procuraduría de la Defensa del Contribuyente (Prodecon) Fiscalía Especializada en Delitos Electorales (federal) Procuradurías o Fiscalías Especializadas en Delitos Electorales en los Estados (local) Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Fecha de nacimiento	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para corroborar datos contenidos en documentos de identificación (RFC, CURP, etc.)	Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Fotografía	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para identificar plenamente a la persona		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal.
Imagen	A través de fotografía y/o video	Dato de identificación Se resguarda en almacenamiento electrónico	Además de identificar plenamente a los trabajadores, se graba en video la participación de estos en la realización de las distintas actividades que desempeñan, videos que son publicados en la plataforma digital del partido	Instituto Nacional Electoral	Los datos personales contenidos en video se conservan permanentemente en la plataforma digital. Una vez cumplida su función -al ser almacenados de manera electrónica- se procede a su destrucción, la cual se realiza a través de la destrucción física.
Registro Federal de Contribuyentes (RFC) con homoclave	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para para identificar a las personas físicas (asalariados) y realizar las retenciones fiscales procedentes	Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público Procuraduría de la Defensa del Contribuyente (Prodecon) Fiscalía Especializada en Delitos Electorales (federal) Procuradurías o Fiscalías Especializadas en Delitos Electorales en los Estados (local) Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Clave Única de Registro de Población (CURP)	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para identificar oficialmente tanto a residentes como a ciudadanos mexicanos de todo el país.	Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.

Estado civil	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para facilitar trámites derivados de derechos en caso de fallecimiento	Instituto Mexicano del Seguro Social	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Lugar de nacimiento	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para corroborar datos en documentos oficiales (CURP)		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Edad	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para asignar las funciones a desempeñar, tomando en cuenta la experiencia	Instituto Mexicano del Seguro Social	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal.
					Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Sexo	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para otorgar los derechos correspondientes (Ej. Incapacidad por maternidad, lactancia, etc.)		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Domicilio	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para establecer contacto con sus familiares en situaciones de riesgo y/o accidente, también para asignar las funciones a desempeñar, privilegiando el lugar de residencia del trabajador.	Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Casa propia o rentada	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento	Para el caso en el que el trabajador tenga asignado un crédito físico		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal.

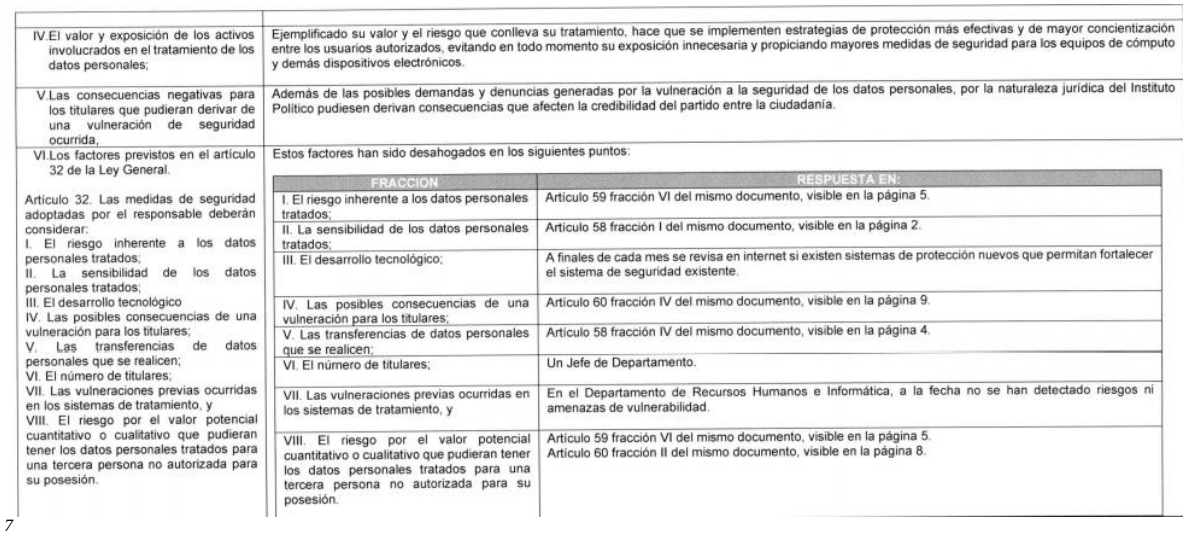
12

Créditos hipotecarios y en su caso números	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento físico y electrónico	Para el caso en el que el trabajador tenga asignado un crédito		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Ingresos	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento físico y electrónico	Para calcular los montos laborales que les corresponden a los trabajadores		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Préstamos	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento físico y electrónico	Para realizar los descuentos respectivos		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Correo electrónico	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para contar con un medio de comunicación institucional	Instituto Mexicano del Seguro Social	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Número de seguridad social	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico y electrónico	Para identificar al trabajador ante el IMSS y realizar las aportaciones por su desempeño laboral.	Instituto Mexicano del Seguro Social	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Número telefónico	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para mantener comunicación directa con los trabajadores	Instituto Mexicano del Seguro Social Bancos	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Escolaridad (estudios realizados, nombres de	A través de un formulario de papel	Dato académico Se resguarda en almacenamiento físico	Para asignar el cargo y funciones a desempeñar, acorde a su experiencia laboral		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan

las escuelas, periodo, número de años cursados y comprobantes)	(solicitud de empleo)				como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Experiencia laboral (nombres de las empresas en que ha laborado, puesto desempeñado , periodo y motivo de separación)	A través de un formulario de papel (solicitud de empleo)	Dato laboral Se resguarda en almacenamiento físico	Para corroborar información del aspirante, en el caso de que las funciones a desempeñar requieran que el perfil del trabajador sea específica y que demuestren experiencia.		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Aspiraciones laborales, títulos, certificados, reconocimientos, constancias, diplomas, cédula profesional	A través de un formulario de papel (solicitud de empleo)	Dato laboral Se resguarda en almacenamiento físico	Para ser considerado de acuerdo a su conocimiento y experiencia, en el supuesto de ascensos laborales y/o asignación de nuevas funciones laborales		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Referencias personales (nombre completo,	A través de un formulario de papel	Dato laboral Se resguarda en almacenamiento físico	Para ser considerado de acuerdo a su conocimiento y experiencia, en el		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan
domicilio, número telefónico);	(solicitud de empleo)		supuesto de ascensos laborales y/o asignación de nuevas funciones laborales		como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Datos familiares (grado de parentesco, nombre, con o sin vida, edad, domicilio y ocupación)	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para comunicarse con los familiares en situaciones de riesgo o accidente laboral		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.

Número de cuenta bancaria	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento físico y electrónico	Para realizar los depósitos de nómina	Banco	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física y electrónica- se procede a su destrucción, la cual se realiza a través de la trituración y destrucción física.
Beneficiario de la cuenta bancaria (nombre, RFC, parentesco y domicilio)	A través de un formulario de papel (solicitud de empleo)	Dato patrimonial Se resguarda en almacenamiento físico	Para que dado el caso, el beneficiario pueda hacerse de los beneficios del trabajador en caso de fallecimiento	Banco	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal.
					Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Documentos de reclutamiento y selección, nombramiento	A través de un formulario de papel (solicitud de empleo)	Dato laboral Se resguarda en almacenamiento físico	Para integrar el expediente laboral		Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.
Firma	A través de un formulario de papel (solicitud de empleo)	Dato de identificación Se resguarda en almacenamiento físico	Para identificar, asegurar o autentificar la identidad del trabajador ó integrante de un órgano de decisión, o como prueba de consentimiento y de verificación de la integridad y aprobación de la información contenida en un documento de carácter legal.	Autoridades jurisdiccionales estatales o federales	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.

DATO PERSONAL SENSIBLE					
DATO	**CAPTURA DE DATOS**	**CLASIFICACION/ALMACENAMIENTO**	**USO/TRATAMIENTO**	**CESION O TRANSFERENCIA DE LOS DATOS A UN TERCERO PARA SU TRATAMIENTO**	**DESTRUCCION**
Huella digital	A través de un formulario	Característica personal	Para identificar plenamente a los trabajadores	Autoridades jurisdiccionales estatales o federales	Los datos personales contenidos de manera general en los expedientes de los trabajadores, se conservan hasta en tanto los titulares laboran en el Instituto Político, y algunos
	de papel (solicitud de empleo)	Se resguarda en almacenamiento físico			en específico -contenidos en comprobantes- se resguardan como mínimo 5 años, de acuerdo a las disposiciones en materia fiscal. Una vez cumplida su función -al ser almacenados de manera física- se procede a su destrucción, la cual se realiza a través de la trituración.



IV. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;	Ejemplificado su valor y el riesgo que conlleva su tratamiento, hace que se implementen estrategias de protección más efectivas y de mayor concientización entre los usuarios autorizados, evitando en todo momento su exposición innecesaria y propiciando mayores medidas de seguridad para los equipos de cómputo y demás dispositivos electrónicos.
V. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida,	Además de las posibles demandas y denuncias generadas por la vulneración a la seguridad de los datos personales, por la naturaleza jurídica del Instituto Político pudiesen derivan consecuencias que afecten la credibilidad del partido entre la ciudadanía.
VI. Los factores previstos en el artículo 32 de la Ley General. Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar: I. El riesgo inherente a los datos personales tratados; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico IV. Las posibles consecuencias de una vulneración para los titulares; V. Las transferencias de datos personales que se realicen; VI. El número de titulares; VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	Estos factores han sido desahogados en los siguientes puntos:

FRACCION	RESPUESTA EN:
I. El riesgo inherente a los datos personales tratados;	Artículo 59 fracción VI del mismo documento, visible en la página 5.
II. La sensibilidad de los datos personales tratados;	Artículo 58 fracción I del mismo documento, visible en la página 2.
III. El desarrollo tecnológico;	A finales de cada mes se revisa en internet si existen sistemas de protección nuevos que permitan fortalecer el sistema de seguridad existente.
IV. Las posibles consecuencias de una vulneración para los titulares;	Artículo 60 fracción IV del mismo documento, visible en la página 9.
V. Las transferencias de datos personales que se realicen;	Artículo 58 fracción IV del mismo documento, visible en la página 4.
VI. El número de titulares;	Un Jefe de Departamento.
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y	En el Departamento de Recursos Humanos e Informática, a la fecha no se han detectado riesgos ni amenazas de vulnerabilidad.
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	Artículo 59 fracción VI del mismo documento, visible en la página 5. Artículo 60 fracción II del mismo documento, visible en la página 8.

7

Como se aprecia en la última fotocaptura, el análisis de brecha realiza 6 reenvíos de información a las personas lectoras, por lo cual, se puntualiza a continuación en que consiste dicha información:

- ***ARTÍCULO 32, FRCC. I, LGPDPPSO. EL RIESGO INHERENTE AL TRATAMIENTO A LOS DATOS PERSONALES TRATADOS:***

  Al respecto, se puntualizó lo siguiente: De acuerdo a las formas en que se resguardan los datos personales, cualquier forma de cancelación, supresión o destrucción de estos obedece a las disposiciones contenidos en la Ley General de Archivos, y que ***se identifica como de riesgo inherente medio****, toda vez que dichos datos permiten conocer la ubicación de la persona y/o cualquier otro que permita identificar a una persona. Por ejemplo, sus dependientes, familiares, beneficiarios, referencias laborales, personales, etc. También son catalogados en esa categoría aquellos datos que permiten identificar el patrimonio de una persona, que incluye entre otros, los saldos bancarios, números de cuenta, bienes muebles e inmuebles, información fiscal, ingresos, créditos, seguros, sueldos y salarios. Son considerados también los datos de autenticación con información a los usuarios, por ejemplo, huellas dactilares, firma autógrafa, fotografías, o identificaciones oficiales. También son catalogados en esta categoría aquellos datos que permiten identificar el patrimonio de una persona, que incluye entre otros los saldos bancarios, números de cuenta, bienes muebles e inmuebles, información fiscal, ingresos, créditos, seguros y salarios. Son considerados también los datos de autenticación con información referente a los usuarios, por ejemplo, huellas dactilares, firma autógrafa, fotografías, identificaciones oficiales. Asimismo, se consideran dentro de este rango los datos jurídicos como litigios y/o cualquier otro tipo de información relativa a que una persona se encuentre sujeta a un procedimiento administrativo seguido de un juicio (…). Por ello, se atiende con sumo cuidado su destrucción, verificando que si se trata de información contenida digitalmente, esta se borre de manera segura y definitiva de los distintos contenedores de información (servidor, nube, etc). Para ello se utilizan dos procedimientos para el borrado de información: el primero es un formato de bajo nivel y es aplicable cuando los equipos son dados de baja definitiva y el segundo, es realizado mediante un borrado local de la información bajo petición en la herramienta EMAS. En caso de datos impresos y contenidos en expedientes, se corrobora*

[7] Se anexa el oficio *CPRF-DRHI-0011/2020,* para mejor referencia.

que una vez destruidos estos no pueden ser armados y que se exponga la información.

- ***ARTÍCULO 32, FRCC. II, LGPDPPSO. LA SENSIBILIDAD DE LOS DATOS PERSONALES TRATADOS:***

- *Se planteó un catálogo de datos personales conforme a su sensibilidad, en el entendido de que la sensibilidad de los datos personales, puede variar dependiendo del contexto que se actualice:*

  - *No sensibles: Nombre completo; fecha de nacimiento; fotografía; registro federal de contribuyentes (RFC) con homoclave; clave única de registro de población (CURP); estado civil; lugar de nacimiento; nacionalidad; edad; sexo; domicilio (propio o rentado); créditos hipotecarios y, en su caso número de los mismos; ingresos; préstamos; correo electrónico; número de seguridad social; número telefónico; escolaridad (estudios realizados, nombres de las escuelas, periodo, número de años cursados y comprobantes); experiencia laboral (nombres de las empresas en que ha laborado, puesto desempeñado, periodo y motivo de separación); aspiraciones laborales, firma, títulos, certificados, reconocimientos, constancias, diplomas y número de folio de cédula profesional; Referencias personales (nombre completo, domicilio y número telefónico); datos familiares (grado de parentesco, nombre, con o sin vida, edad, domicilio y ocupación); número de cuenta bancaria; beneficiario de la cuenta bancaria (nombre, RFC, parentesco y domicilio); documentos de reclutamiento y selección, así como nombramiento; información fiscal; descuentos por orden judicial (puede ser sensible).*

  - *Sensibles: Huella dactilar; imagen; clave de elector (en el caso del Órgano Técnico Electoral).*

- ***ART. 32 FRCC. III, LGPDPPSO. EL DESARROLLO TECNOLÓGICO.***

- *El DRHI de la CPRF del PRD, manifestó que a finales de cada mes se revisa si en Internet existen productos y servicios que puedan mejorar la calidad de los ya implementados para garantizar las medidas de seguridad técnicas en este Instituto político. Los equipos de cómputo son renovados periódicamente y ello implica utilizar los programas de antivirus recomendados e incluidos por el proveedor, por otra parte, el personal de ese Departamento, están siempre, en su horario de trabajo, disponibles para atender cualquier consulta técnica, o darse el caso, incidencias.*

- ***ART. 32, FRCC. IV, LGPDPPSO LAS POSIBLES CONSECUENCIAS SOBRE VULNERACIONES A LOS DATOS PERSONALES DE LAS PERSONAS QUE OSTENTEN SU TITULARIDAD.***

  Al respecto, en la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, se advirtió que en caso de que pudiera vulnerar o estar en riesgo de amenaza hacia los datos personales, las personas titulares podrían sufrir consecuencias negativas, por ejemplo, la celebración de un contrato sin su consentimiento, inclusive cobro por algún servicio, no obstante, también es posible añadir, que podría ocurrir una suplantación de identidad que podría encontrase conexa con otras afectaciones, por ejemplo, dañar la imagen o generar escenarios adversos en la vida interna del Partido de la Revolución Democrática, incluso, hay datos personales, que pueden poner en peligro derechos humanos como el anonimato, la integridad psicológica, física, e incluso generar discriminación.

Lo anterior es así, derivado de que los datos patrimoniales, conjuntamente con los de identificación, de contacto y de residencia, pueden ser utilizados por personas con malas intenciones para causar daños patrimoniales, pero no solo mediante la celebración de actos jurídicos recurriendo a falsas identidades, sino recurriendo incluso mediante conductas delictivas como al extorsión o el secuestro. Finalmente y, no es un tema menor, la suplantación de identidad también puede afectar la reputación de las personas.

Según el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en el año 2017, se registraron 78.989 reclamaciones bancarias por un posible Robo de Identidad, reclamando un monto total por $2,127,025,853 pesos mexicanos, cifra que desafortunadamente ha registrado una tendencia a aumentar con el paso del tiempo.[8]

- ***ARTÍCULO 32, FRCC. V LGPDPPSO. LAS TRANSFERENCIAS DE DATOS PERSONALES QUE PUDIERAN REALIZARSE***

Son las siguientes: Autoridades electorales, tanto en el Poder Judicial de la Federación y en las entidades federativas, como los poderes ejecutivos de dichos ámbitos de competencia; autoridades hacendarias federales y locales; autoridades de seguridad social; el Partido de la Revolución Democrática en las entidades federativas y, con relación a la Campaña de Salud # Yo Te Defiendo, los siguientes entes, autoridades y personas físicas:

A. PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA.

** Partido de la Revolución Democrática en Aguascalientes;*
** Partido de la Revolución Democrática en Baja California;*
** Partido de la Revolución Democrática en Baja California Sur;*
** Partido de la Revolución Democrática en Campeche;*
** Partido de la Revolución Democrática en Chiapas;*
** Partido de la Revolución Democrática en Chihuahua;*
** Partido de la Revolución Democrática en Coahuila de Zaragoza;*
** Partido de la Revolución Democrática en Colima;*
** Partido de la Revolución Democrática en Durango;*
** Partido de la Revolución Democrática en Estado de México;*
** Partido de la Revolución Democrática en Guanajuato;*
** Partido de la Revolución Democrática en Guerrero;*
** Partido de la Revolución Democrática en Hidalgo;*
** Partido de la Revolución Democrática en Jalisco;*
** Partido de la Revolución Democrática en Michoacán de Ocampo;*
** Partido de la Revolución Democrática en Morelos;*
** Partido de la Revolución Democrática en Nayarit;*
** Partido de la Revolución Democrática en Nuevo León;*
** Partido de la Revolución Democrática en Oaxaca;*

[8] http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf

** Partido de la Revolución Democrática en Puebla;*
** Partido de la Revolución Democrática en Queretaro;*
** Partido de la Revolución Democrática en Quintana Roo;*
** Partido de la Revolución Democrática en San Luis Potosí;*
** Partido de la Revolución Democrática en Sinaloa;*
** Partido de la Revolución Democrática en Sonora;*
** Partido de la Revolución Democrática en Tabasco;*
** Partido de la Revolución Democrática en Tamaulipas;*
** Partido de la Revolución Democrática en Tlaxcala;*
** Partido de la Revolución Democrática en Veracruz de Ignacio de la Llave;*
** Partido de la Revolución Democrática en Yucatán;*
** Partido de la Revolución Democrática en Zacatecas;*
** Juzgados de Distrito del Poder Judicial de la Federación;*
** Tribunales Unitarios de Circuito del Poder Judicial de la Federación;*
** Tribunales Colegiados de Circuito del Poder Judicial de la Federación;*
** Salas de la Suprema Corte de Justicia de la Nación;*
** Pleno de la Suprema Corte de Justicia de la Nación;*
** Consejo de la Judicatura Federal;*
** Instituto de la Judicatura Federal;*

B. AUTORIDADES DE SALUD:

Federales:

- *Administración del Patrimonio de la Beneficencia Pública*
- *Centro Nacional de Equidad de Género y Salud Reproductiva*
- *Centro Nacional de Excelencia Tecnológica en Salud*
- *Centro Nacional de la Transfusión Sanguínea*
- *Centro Nacional de Programas Preventivos y Control de Enfermedades*
- *Centro Nacional de Trasplantes*
- *Comisión Nacional contra las Adicciones*
- *Centro Nacional para la Prevención y el Control del VIH/SIDA*
- *Centro Nacional para la Salud de la Infancia y la Adolescencia*
- *Comisión Federal para la Protección contra Riesgos Sanitarios*
- *Comisión Nacional de Arbitraje Médico*
- *Comisión Nacional de Bioética*
- *Comisión Nacional de Protección Social en Salud*
- *Servicios de Atención Psiquiátrica*
- *Centro Regional de Alta Especialidad de Chiapas*
- *Hospital General "Dr. Manuel Gea González"*
- *Hospital General de México "Dr. Eduardo Liceaga"*
- *Hospital Infantil de México Federico Gómez*
- *Hospital Juárez de México*
- *Hospital Regional de Alta Especialidad de Ciudad Victoria "Bicentenario 2010"*
- *Hospital Regional de Alta Especialidad de Ixtapaluca*
- *Hospital Regional de Alta Especialidad de la Península de Yucatán*
- *Hospital Regional de Alta Especialidad de Oaxaca*
- *Hospital Regional de Alta Especialidad del Bajío*
- *Instituto Nacional de Cancerología*

- *Instituto Nacional de Cardiología Ignacio Chávez*
- *Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán*
- *Instituto Nacional de Enfermedades Respiratorias Ismael Cosío Villegas*
- *Instituto Nacional de Geriatría*
- *Instituto Nacional de Medicina Genómica*
- *Instituto Nacional de Neurología y Neurocirugía Manuel Velasco Suárez*
- *Instituto Nacional de Pediatría*
- *Instituto Nacional de Perinatología Isidro Espinosa de los Reyes*
- *Instituto Nacional de Psiquiatría Ramón de la Fuente Muñiz*
- *Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra*
- *Instituto Nacional de Salud Pública*
- *Sistema Nacional para el Desarrollo Integral de la Familia*
- *Instituto Mexicano del Seguro Social*
- *Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra*
- *Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado*

Aguascalientes

- *Instituto de servicios de Salud de Estado de Aguascalientes*
- *Instituto de Seguridad y Servicios Sociales para los Servidores Públicos del Estado de Aguascalientes (ISSSSPEA)*

Baja California

- *Instituto de Psiquiatría del Estado de Baja California*
- *Instituto de Seguridad y Servicios Sociales de los Trabajadores del Gobierno y Municipios del Estado de Baja California*
- *Instituto de Servicios de Salud Pública del Estado de Baja California*
- *Régimen de Protección Social en Salud de Baja California*
- *Secretaría de Salud*

Baja California Sur

- *Instituto de Servicios de Salud*
- *Secretaría de Salud*
- *Régimen Estatal de Protección Social En Salud (REPSS-BCS)*

Campeche

- *Instituto de Servicios Descentralizados de Salud Pública del Estado de Campeche*
- *Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Campeche*
- *Secretaria de salud*
- *Régimen Estatal de Protección Social en Salud*

Coahuila de Zaragoza

- *Secretaría de Salud*
- *Servicios de Salud*
- *Instituto de Servicios, Rehabilitación y educación Especial e Integral del Estado de Coahuila (ISREEI)*

Colima

- *Laboratorio Estatal de Salud Publica*
- *Régimen Estatal de Protección Social en Salud del Estado de Colima (REPSS)*
- *Servicios de Salud del Estado*
- *Secretaría de Salud y Bienestar Social*
- *Centro Estatal de Transfusión Sanguínea*

Chiapas

- *Régimen Estatal de Protección Social en Salud*
- *Secretaría / Instituto de Salud*
- *Instituto de Seguridad Social de los Trabajadores del Estado de Chiapas*
- *Centro Estatal de Trasplantes del Estado de Chiapas*

Chihuahua

- *Instituto Chihuahuense de la Salud*
- *Centro Estatal de Protección Social en Salud*
- *Secretaría de Salud*
- *Servicios de Salud de Chihuahua*

Ciudad de México

- *Secretaría de Salud*
- *Servicios de Salud Publica de la Ciudad de México*
- *Régimen de Protección Social en Salud de la Ciudad de México*

Durango

- *Régimen de Protección Social en Salud*
- *Secretaria de Salud del Estado de Durango (SSD)*

Guanajuato

- *Centro de Rehabilitación e inclusión infantil Guanajuato*

Guerrero

- *Secretaría de Salud*
- *Régimen Estatal de Protección Social en Salud en Guerrero (Seguro Popular)*
- *Instituto Estatal de Cancerología*
- *Instituto Estatal de Oftalmología*
- *Hospital de la Madre y el niño Guerrerense*
- *Hospital de la Madre y el niño Indígena Guerrerense*

Hidalgo

- *Centro de rehabilitación e inclusión infantil Teletón Hidalgo*

Jalisco

- *Centro de estimulación para Personas con Discapacidad Intelectual*

Michoacán de Ocampo

- *Régimen Estatal de Protección Social en Salud de Michoacán de Ocampo*
- *Secretaría de Salud de Michoacán*

Morelos

- *Hospital del Niño Morelense*
- *Régimen Estatal de Protección Social en Salud de Morelos*

Nayarit

- *Instituto para la Mujer Nayarita*
- *Régimen Estatal de Protección Social en Salud*

Nuevo León

- *Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Nuevo León (ISSSTELEON) (OPD)*
- *Instituto Estatal de las Mujeres (OPDPC)*
- *Instituto Estatal de las Personas Adultas Mayores*

Oaxaca

- *Hospital de la Niñez Oaxaqueña*
- *Comisión Estatal de Arbitraje Médico*
- *Consejo Estatal para la Prevención y Control del Sida*

Querétaro

- *Instituto Municipal de la Mujer Corregidora*

- *Instituto Municipal de la Mujer de Pedro Escobedo*
- *Instituto Queretano de las Mujeres*

Quintana Roo

- *Instituto Quintanarroense de la Mujer*

San Luis Potosí

- *Hospital Central "Dr. Ignacio Morones Prieto*

Tabasco

- *Instituto de Seguridad Social del Estado de Tabasco (ISSET)*
- *Instituto General de las Mujeres*

Tamaulipas

- *Instituto de la Mujer Tamaulipeca*
- *Instituto de previsión y seguridad social del estado de Tamaulipas*

Tlaxcala

- *Comisión estatal para la protección contra riesgos sanitarios*
- *Instituto Tlaxcalteca para personas con discapacidad*

Veracruz de Ignacio de la Llave

- *Secretaria de salud*
- *Régimen Estatal de Protección Social en Salud*

Yucatán

- *Hospital comunitario de Peto, Yucatán*
- *Hospital comunitario de Ticul, Yucatán*
- *Hospital General de Tekax*
- *Hospital de la Amista de Corea*
- *Centro Estatal de Trasplante de Yucatán*
- *Instituto de seguridad social para los trabajadores del estado de Yucatán*

Zacatecas

- *Régimen Estatal de Protección Social en Salud*

C. AUTORIDADES DEL PODER JUDICIAL:

- El Supremo Tribunal de Justicia; la Sala Administrativa; los Juzgados de Primera Instancia; Juzgados de Control; de Juicio Oral y de Ejecución; el Consejo de la Judicatura Estatal; el Instituto de Capacitación; y la Controlaría Interna; ***en el estado de Aguascalientes;***

- *Tribunal Superior de Justicia actuando en Pleno o en Salas; Consejo de la Judicatura,* ***así como toda autoridad de salud en el Estado de Baja California;***

- Tribunal Superior de Justicia y Consejo de la Judicatura; Jueces de Control, Tribunal Unitario de Enjuiciamiento; el Juez de Ejecución, Especializados en el Sistema Integral de Justicia Penal, ***en el estado del Estado de Baja California Sur****;*

- Honorable Tribunal Superior de Justicia; Jueces de primera instancia; Jueces de control; tribunales de enjuiciamiento; jueces de ejecución de sanciones; jueces de cuantía menor; jueces mixtos; jueces auxiliares; jueces conciliadores; Consejo de la Judicatura Local del Poder Judicial ***en el estado del Estado de Estado de Campeche****;*

- Supremo Tribunal de Justicia; el Consejo de la Judicatura; Juzgados de Primera Instancia; Juzgado de Paz y Conciliación; Juzgados de Paz y Conciliación Indígena; y Juzgados Municipales ***en el estado del Estado de Chiapas;***

- Tribunal Superior de Justicia que funciona en Pleno o en Salas; y Consejo de la Judicatura ***en el estado del Estado de Chihuahua;***

- Tribunal Superior de Justicia; Tribunales Especializados – Tribunal de Conciliación y Arbitraje -; Tribunales Distritales; Juzgados de Primera Instancia; Juzgados letrados; y Consejo de la Judicatura ***en el estado de Coahuila de Zaragoza****;*

- Supremo Tribunal de Justicia; Juzgados de Primera Instancia; Juzgados Especializados […]; Juzgados de Control; Tribunales de Enjuiciamiento; Juzgados de Ejecución de Penas y Medidas de Seguridad; y Juzgados de Menor Cuantía; Centro Estatal de Justicia Alternativa ***en el estado de Colima.***

- Tribunal Superior de Justicia; Juzgados de Primera Instancia y Auxiliares, los Jueces de Control, Tribunales de Enjuiciamiento; los Juzgados de Ejecución y el Tribunal Laboral Burocrático; Centro de Justicia Alternativa; Juzgados Municipales; los Juzgados de Primera Instancia y Auxiliares; y Juzgados Municipales y el Consejo de la Judicatura ***en el estado de Durango.***

- Tribunal Superior de Justicia; Consejo de la Judicatura; juzgados y tribunales de primera instancia; tribunales laborales; y juzgados de cuantía menor ***en el Estado de México.***

- Supremo Tribunal de Justicia de Guanajuato; Consejo del Poder Judicial; juzgados de primera instancia, especiales o auxiliares; jueces de control; así como tribunales de enjuiciamiento ***en el estado de Guanajuato.***

- Tribunal Superior de Justicia; Consejo de la Judicatura; Juzgados de Primera Instancia; Juzgados de Paz; órganos de administración de justicia ***en el estado de Guerrero.***

- Tribunal Superior de Justicia y Jueces del Fuero Común; Tribunal Fiscal Administrativo; Consejo de la Judicatura, Juzgados de primera instancia, auxiliares, de control, o tribunales de enjuiciamiento ***en el Estado de Hidalgo.***

- Supremo Tribunal de Justicia; Tribunal de lo Administrativo; Juzgados de Primera Instancia, Especializados y Mixtos; Juzgados Menores; Juzgados de Paz; y Jurado Popular ***en el estado de Jalisco;***

*- Supremo Tribunal de Justicia del Estado; juzgados de Primera instancia; juzgados Especializado en Adolecentes; juzgados Menores; juzgados Comunales; y Consejo del Poder Judicial del Estado****, en Michoacán de Ocampo;***

- Tribunal Superior de Justicia; Consejo de la Judicatura Estatal; Juzgados de Primera Instancia; Juzgados Menores; Juzgados de Paz; Jurado Popular; y Árbitros ***en el Estado de Morelos;***

- Tribunal Superior de Justicia; Consejo de la Judicatura; y Juzgados de Primera Instancia ***en el estado de Nayarit****;*

- Tribunal Superior de Justicia; Juzgados de lo Civil; Juicio Civil Oral; Juzgados de lo Familiar, de lo Familiar Oral; de Ejecución Familiar Oral; Juzgados de lo Penal; Juzgados de Preparación de lo Penal; Juzgados de Control; Juicio Oral Penal; Juzgados de Ejecución de Sanciones Penales; Juzgados de Jurisdicción Concurrente; Juzgados de Juicio Oral Mercantil; Juzgados de Jurisdicción Mixta; Juzgados Supernumerarios; Juzgados Menores ***en el estado de Nuevo León****.*

- Pleno del Tribunal Superior de Justicia en el Estado; Salas Especializadas en razón de la materia; Tribunal de lo Contencioso Administrativo y de Cuentas; y Juzgados de primera instancia ***en el estado de Oaxaca****;*

- Tribunal Superior de Justicia; Consejo de la Judicatura del Poder Judicial del Estado; Juzgados de Primera Instancia; y Juzgados Indígenas ***en el estado de Puebla;***

- Tribunal Superior de Justicia; Consejo de la Judicatura; Juzgados de primera instancia; y Juzgados Menores ***en el estado de Querétaro****;*

- Tribunal Superior de Justicia; Juzgados de Primera Instancia; y Juzgados de Paz; Consejo de la Judicatura del Estado, ***en Quintana Roo****;*

- Supremo Tribunal de Justicia; Jueces de Primera Instancia; Juzgados Penales; Juzgados de Control; Tribunales de Juicio Oral; Juzgados de Ejecución de Sentencia y Jueces Auxiliares ***en el estado de San Luis Potosí;***

- Supremo Tribunal Justicia; Salas de Circuito; Juzgados de Primera Instancia; y Juzgados Menores ***en el estado de Sinaloa****;*

- Supremo Tribunal de Justicia; Tribunales Regionales de Circuito; Juzgado de Primera Instancia; y Juzgados Locales ***en el estado de Sonora****;*
- Tribunal Superior de Justicia, Pleno del Tribunal Superior de Justicia; Salas en materia civil, penal, y Salas especializadas en materia de oralidad, de ejecución y de justicia para adolescentes ***en el estado de Tabasco****;*
- Pleno del Tribunal Supremo de Justicia; Salas Numerarias y Auxiliares; Jueces de Primera Instancia; Jueces Menores; Jurado Popular; y Árbitros ***en el estado de Tamaulipas.***
- Tribunal Superior de Justicia funcionando en Pleno y Salas; Consejo de la Judicatura; Juzgados de lo Civil; Juzgado de lo Penal; Juzgados de Ejecución de Sanciones Penales; Juzgados de Jurisdicción Mixta; Juzgados de Garantías de Adolescentes; Juzgados de Administración de Justicia para adolescentes; y Centro Estatal de Justicia Alternativa; Juzgados de primera instancia; y Tribunal de Justicia Administrativa ***del estado de Tlaxcala****.*
- Tribunal Superior de Justicia; Tribunal de lo Contencioso Administrativo; Tribunal de Conciliación y Arbitraje; juzgados de primera instancia; Juzgados de procesos y procedimientos penales orales, Juzgados menores; Juzgados Municipales; Juzgados de comunidad; y organismos administrativos ***en el estado de Veracruz de Ignacio de la Llave.***
- Tribunal Constitucional; Tribunal Superior de Justicia; el Tribunal de los Trabajadores al Servicio del Estado y de los Municipios, los tribunales y juzgados de primera instancia y los juzgados de paz ***en el estado de Yucatán****;*
- Tribunal Superior de Justicia; Tribunal Especializado en Justicia para Adolescentes; y Juzgados de Primera Instancia, que podrán ser Civiles, Familiares, Mercantiles, Mixtos de Control y Tribunal de Enjuiciamiento; de Ejecución de Sanciones ***en el estado de Zacatecas.***

D. Personas físicas

Aquellas que de manera voluntaria le auxilien para la presentación, y seguimiento a su amparo en calidad de responsables quienes se comprometerán a velar por sus datos personales en el marco de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- ***ART. 32, FRCC. VI. LGPDPPSO. NÚMERO DE PERSONAS TITULARES DE DATOS PERSONALES***

Se subdividen en las siguientes hipótesis: a) militantes; b) servidores intrapartidarios adscritos a algún órgano estatutario; c) particulares que acuden a ejercer su derecho de acceso a la información; d) personas que acuden a buscar apoyo en el marco de la Campaña de Salud #Yo Te Defiendo; e) personas que operan como proveedores de productos y servicios; f) personas que ingresan a los inmuebles del Partido de la Revolución Democrática para cualquier otro propósito. Al día que se emite este informe, no se tiene una cifra actualizada del universo de posibles titulares de datos personales, pero se le invita a consultar el Portal de Transparencia del Partido de la Revolución Democrática: https://transparencia-prd.org.mx/

- ***ART. 32, FRCC. VII. LAS VULNERACIONES PREVIAS OCURRIDAS EN EL TRATAMIENTO DE DATOS PERSONALES.***

No se han reportado a esta Unidad de Transparencia vulneraciones de datos personales.

- ***ART. 32, FRCC. VIII. EL RIESGO POR EL VALOR POTENCIAL CUANTITATIVO O CUALITATIVO QUE PUDIERAN TENER LOS DATOS PERSONALES TRATADOS PARA UNA TERCERA PERSONA NO AUTORIZADA PARA SU POSESIÓN.***

De conformidad con la Frcc. II del artículo 60 de la LGPDPPSO, al respecto, de los informe

recibidos en esta Unidad de Transparencia, se advierte lo siguiente:

"El valor de los datos personales es considerado de riesgo MEDIO, agrupándose de la siguiente forma:

a) *Identificativos: Nombre complete, domicilio, fecha de Nacimiento, edad, número telefónico, estado civil, lugar de Nacimiento, nacionalidad, sexo, fotografía, registro federal de contribuyentes, clave única de Registro de Población, […] firma y en el caso del Órgano Técnico Electoral, clave de elector.*

b) ***Datos electrónicos:*** *correo electrónico*

c) ***Datos académicos:*** *Títulos, certificados, reconocimientos, constancias, diplomas, cédula profesional*

d) ***Datos laborales:*** *Aspiraciones laborales, documentos de recluamiento y selección, estudios realizados, nombres de las escuelas (donde estudió la persona titular de datos personales), periodo, número de años cursados, comprobantes, nombramiento, referencias laborales, número de seguro social, experiencia laboral, referencias personales, datos familiares.*

e) ***Datos patrimoniales:*** *Créditos hipotecarios, número de cuenta bancaria, beneficiario de la cuenta bancaria, información fiscal, descuentos por orden judicial, préstamos e ingresos.*

f) ***Datos biométricos:*** *Huella digital.*

De acuerdo a la información contenida en el "Estudio sobre el valor económico de los datos personales", elaborado para la Asociación Mexicana de Internet A.C. (AMIPCI), ahora Asociación Mexicana de Internet.mx, y la Secretaría de Economía, en una encuesta realizada donde el valor es de 0 a 10, se aprecian cifras que muestran el análisis comparativo de los principales tipos de datos, ya sean sensibles o no sensibles, a los cuales los individuos participantes les asignaron una mayor importancia, como resultado de la pregunta `… en una escala del 0 al 10, para cada uno de los siguientes datos… califique el nivel de importancia para usted mediante el indicador preservar/cuidar´.

Se retoman dichos resultados en un intento de mostrar el valor que pudiese otorgarse a los datos personales […] destacando que el promedio de los datos no sensibles, donde se incluyeron los datos financieros y patrimoniales, es de 7.5 en una escala de valoración de 0 a 10, siendo superior al promedio de los datos sensibles del orden del 6.6.

Es importante destacar que los datos financieros y patrimoniales, son los datos a los cuales los individuos participantes, les asignaron una mayor importancia con una calificación de 8.7, seguido de los datos biométricos con 8.1, y los datos legales con una evaluación de 7.8

En los datos de identificación y contacto, se obtuvo un promedio de 7.8 donde la firma electrónica es el dato calificado como más valioso con 9.2, seguido de la firma autógrafa 9.1 y los datos de domicilio 9.1. Le siguen en importancia los números telefónicos, tanto el teléfono particular como el número de teléfono celular. Los datos de identificación más comunes como edad, nacionalidad y estado de civil son los considerados de menor importancia.

En lo referente a los datos laborales, se obtuvo un promedio de 7.4, observándose una mayor calificación a los datos e información generada durante los procesos de reclutamiento, selección y confrontación con 7.9.

Los datos académicos (sic)se observó una calificación promedio de 7.6. Los individuos participantes consideran de mayor importancia el dato de la cédula profesional con un 8.4 de calificación, seguida de los títulos y certificados con una calificación de 7.7.

Los datos financieros o patrimoniales son los que significaron una mayor importancia para los individuos participantes con una calificación promedio de 8.7. Se destacan por su importancia los datos relacionados con información adicional de la tarjeta, por ejemplo: fecha de vencimiento, código de seguridad, datos de la banda magnética y PIN, con una calificación de 9.2 y de los números de tarjetas de crédito con 9.1.

[…]

Según el Departamento de Recursos Humanos e Informática del Partido de la Revolución Democrática, el ciclo de vida depende en gran medida de los efectos para los cuales sea necesario su uso; esto es, hay datos que por las facultades y atribuciones de ese Departamento, son utilizados para realizar el pago de salarios, otros donde su ciclo de vida depende de su periodo de vigencia (por ejemplo, los ya descritos que se ubican en la credencial de elector), la cual es necesario renovar para que surta los efectos de identificación y/o emisión de voto. Hay algunos otros datos cuyo ciclo de vida pareciera inalterable, pero en este Departamento cobran gran importancia, tal y como lo es un cambio de residencia, donde el domicilio del trabajador fue aportado al momento de ingreso y es el que quedó registrado ante el IMSS y es necesario el cambio previniendo cualquier aclaración. El ciclo de vida de los datos personales utilizados en ese Departamento, está descrito en las fotocapturas sitas en líneas anteriores.

- *Ahora bien, es importante resaltar las aportaciones que el Departamento Jurídico, adscrito a la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática:*

"Datos personales	*Valor*
Nombre completo de representante legal	*Indispensable para identificar a quien suscribe el contrato en representación de la persona moral.*
Número de instrumento notarial	*Necesario contar con domicilio para oír y recibir notificaciones relacionadas con las obligaciones contraídas en el contrato celebrado con el PRD.*
Registro	*Es recabado con la finalidad de identificar quien*

Federal de Electores R.F.C.	*emite facturas al PRD, y correlacionadas con la información a cargo del área contable.*
Número de Registro Nacional de Proveedores	*Para poder celebrar contratos de conformidad con lo establecido en el Reglamento de Fiscalización del INE*
Correo electrónico *Número telefónico*	*Necesario para debida integración del expediente como proveedor y/o prestador de servicios del Partido, y mantener comunicación directa con la persona moral.*
Firma autógrafa de representante legal	*Signo gráfico con el cual, el representante legal otorga certeza y eficacia a los contratos con el partido, ya que constituye la aceptación de su contenido.*

En relación con lo anterior, este Departamento Jurídico cuenta con activos como la contratación de un servicio de Internet para operar el correo electrónico, material para formar los expedientes respectivos y anaqueles, los cuales se encuentren involucrados en el tratamiento de datos personales."

Para conocer la información provista al respecto por otros órganos intrapartidarios, se remite a la persona lectora a la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, que puede consultarse mediante el siguiente hipervínculo: https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2019/10S_Ordinaria_29-10-2019.pdf

- *Esta Unidad de Transparencia, con relación a la fracción I del artículo 60 de la LGPDPPSO, en su momento refirió que las mejores prácticas que el PRD pone en práctica, son tomadas, entre otras fuentes de las Guías que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, pone a disposición del público general mediante su Portal de Internet.*

Análisis de brecha

Realizar un análisis de brecha, es una obligación que tiene el Partido de la Revolución Democrática con relación a la integración del Documento de Seguridad, a continuación, se ofrecen capturas de pantalla de las manifestaciones del Departamento de Recursos Humanos e Informática de la Coordinación del Patrimonio y Recursos Financieros del Partido de la Revolución Democrática, ***que resultan coincidentes con las provistas por otros órganos intrapartidarios:***

I. Las medidas de seguridad existentes y efectivas;	I. **Medidas de seguridad fisicas:** El Partido de la Revolución Democrática cuenta con una recepción que controla la entrada de personal y visitantes al edificio, para cuyo acceso es necesario que el personal porte su credencial institucional y, en el caso de visitantes se realice un registro de ingreso en el cual se le solicita nombre, motivo de la visita, a quien visita, oficina y piso al que accede, hora de entrada, hora de salida y firma. Una vez realizado el registro, se le proporciona un gafete con la leyenda "visitante" para que tenga paso libre al edificio. Asimismo, se le solicita al visitante que refiera si porta algún equipo electrónico (laptop, tableta, etc.) y/o algún otro aparato. Asimismo, en la oficina que ocupa el Departamento de Recursos Humanos e Informática se encuentra una recepción, en la cual la secretaria canaliza la petición del visitante al servidor partidista y éste a su vez autoriza el ingreso de dicha persona. Las oficinas que se encuentran dentro de este Departamento, cuentan con cerrojo y usualmente se encuentran abiertas, salvo al momento de concluir labores se cierran, así como las gavetas donde se resguardan los expedientes (físicos y electrónicos) y archivos que contienen datos personales. Adicionalmente, se cuenta con las siguientes medidas: 1. Videovigilancia en todo el interior del edificio y periferia externa 2. Acceso restringido a lugares distintos al lugar de visitas 3. Control de ingreso y salida de muebles y documentos 4. Inclusión de cláusula de confidencialidad de información en los contratos 5. Destrucción total de documentos **Medidas de seguridad técnicas:** Los datos personales se encuentran concentrados en la computadora instalada en la oficina del Jefe de Departamento de Recursos Humanos e Informática, ubicada al fondo de la estancia general, de lado izquierdo mirando de frente la Avenida Benjamín Franklin. Asimismo, se tiene respaldo en el servidor, la nube (Tier 3+) y discos duros externos cifrados para cuyo acceso es necesario contar con claves, las cuales se encuentran solamente en conocimiento del Jefe de Departamento y el Profesionista Especializado en funciones de coordinador de informática. Asimismo, se cuenta con las siguientes medidas: 1. Medidas de política de contraseñas. Se revisa y actualiza semestralmente la configuración de los sistemas. 2. Baja de cuentas de personal que ya no labora en el Instituto. 3. Uso de contraseñas para el acceso a los sistemas informáticos. Cada seis meses se obtiene un reporte de todos los usuarios del sistema operativo por medio del cual se administran todas las cuentas que se dan de alta en el Senado para otorgar a la red, y validar que, en el campo correspondiente a la contraseña, no estén vacíos, a fin de asegurar el uso de contraseñas en todos los casos. 4. Servidor resguardado bajo medidas de seguridad ambientales, de acceso, de temperatura, etc. 5. Implementación y monitoreo de vulnerabilidad de red por medio de herramientas especializadas. 6. Acceso a los sistemas conforme a procedimiento de administración de usuarios. 7. Borrado de información que reside en los equipos de cómputo. **Medidas de seguridad administrativa:** Por lo que hace a los datos personales en expedientes, estos se mantienen solamente en uso del personal autorizado y fuera del alcance de los demás trabajadores y, por lo que hace a los archivos electrónicos, estos son motivo de continuas actualizaciones de antivirus y demás sistemas de seguridad y protección.
II. Las medidas de seguridad faltantes, y	Dado que hasta el momento no se presentado ni amenazas ni riesgos de vulnerabilidad a los archivos físicos ni electrónicos, se considera que las medidas de seguridad implementadas cumplen con los objetivos.
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente	Por parte del área de informática, se consulta mensualmente en internet los nuevos sistemas de seguridad para equipos de cómputo, y si existe alguno que ofrezca mayores medidas de protección, se solicita el recurso para su compra; además de aplicar los parches de seguridad proporcionada por el sistema operativo para corregir vulnerabilidades detectadas.

Para conocer la información provista al respecto por otros órganos intrapartidarios, se remite a la persona lectora a la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, que puede consultarse mediante el siguiente hipervínculo: https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2019/10S_Ordinaria_29-10-2019.pdf

3- Mecanismos de monitoreo

A continuación, se pueden apreciar las manifestaciones que el Departamento de Recursos Humanos y Recursos Financieros de la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática, realizó con relación a los mecanismos de monitoreo:

Fracción VI.- Los mecanismos de monitoreo y revisión de las medidas de seguridad. Fracción VII, Art. 33. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y	
Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua. Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:	
I.Los nuevos activos que se incluyan en la gestión de riesgos;	La entrada en vigor de la NOM-035-STPS-2018 a partir del 23 de octubre de 2019, dispone que este sujeto obligado deberá establecer los elementos para identificar, analizar y prevenir los factores de riesgo psicosocial, así como para promover un entorno organizacional favorable en los centros de trabajo. Estos nuevos activos deberán considerarse en la gestión de riesgos, motivo por el cual continuamente serán monitoreados dichos datos.
II.Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	Dichas modificaciones deberán atender las disposiciones contenidas en la Ley General de Protección de Datos en Posesión de Sujetos Obligados y la Ley General de Archivos; sin embargo, todos los documentos físicos que contienen datos personales se digitalizan previniendo riesgos (intencionales o no), actividad que se realiza cotidianamente.
III.Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	-Contraseñas débiles o que no se modifiquen periódicamente -Carecer de convenios de confidencialidad con el personal interno -No accesibilidad al mantenimiento de hardware, para el debido resguardo de archivos electrónicos
IV.La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	Cada ronda de mantenimiento a los equipos de cómputo, se analizan los resultados y se determinan las medidas a seguir para evitar que se generen o aumenten las posibles vulnerabilidades.
V.Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	Cada ronda de mantenimiento a los equipos de cómputo, se analizan los resultados y se determinan las medidas a seguir para evitar que se presenten posibles amenazas.
VI.El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos	En una bitácora por cada equipo de cómputo, se detallan todos aquellos registros que pudiesen significar un riesgo para la confidencialidad de los datos personales, valorándose periódicamente si con las medidas adoptadas preventivamente, disminuyen posibles amenazas y/o que se generen nuevas o se incrementen las vulnerabilidades existentes
VII.Los incidentes y vulneraciones de seguridad ocurridas. Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión	Hasta el momento el sistema de gestión ha resultado del todo eficaz y eficiente, ya que no se han presentado incidentes ni vulneraciones. Sin embargo, se elaborará un programa de auditoría el cual tendrá como objetivo monitorear y verificar los resultados del sistema de gestión obtenidos al día de hoy.

- ***Programa de Trabajo***

Esta Unidad de Transparencia, en su momento refirió que en marzo de 2019, el Comité de Transparencia del Partido de la Revolución Democrática, sesionó para presentar un plan anual de capacitación, mediante la cual, fue posible escuchar distintos puntos de vista los integrantes de los diversos órganos intrapartidarios de este Instituto político, además, fue posible tener diversas reuniones con cada órgano intrapartidario para elaborar los insumos que finalmente darían como fruto este documento de transparencia proactiva. Lo expuesto, será abordado mediante el siguiente punto de análisis.

- ***Sistema de Gestión de Protección de Datos Personales del Partido de la Revolución Democrática***

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha puesto de manifiesto la importancia de la generación de un Sistema de Gestión de Protección de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), lo anterior, en el marco del artículo 34 de la Ley General de Protección de Datos Personales, en Posesión de los Sujetos Obligados.

De conformidad con el artículo 2º Frcc. XIV de la LGPDPPSO, el Sistema de Gestión de Datos Personales es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas, administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee. Dicho instrumento puede integrarse siguiendo las siguientes fases:

a) Fase 1. Planear el SGPDP[9]:

a. Paso 1. Establecer el Alcance y los Objetivos[10];

b. Paso 2. Elaborar una Política de Gestión de Datos Personales[11];

c. Paso 3. Establecer funciones y obligaciones[12].

d. Paso 4. Elaborar un inventario de datos personales.[13]

e. Paso 5. Realizar un Análisis de Riesgo de Datos Personales (ARDP). [14]

Para realizar un ARDP, es posible cumplir con los siguientes pasos: 1. Identificar los

---

[10] Se deben tomar en cuenta factores contractuales, legales y regulatorios, así como el modelo de negocio/trabajo, tecnológicos. Es importante identificar plenamente el perfil de los titulares de datos personales, responsable / sujetos obligados, encargados, custodios, alta gerencia.

[11] Para elaborar una política de gestión de datos personales, es importante tomar en cuenta ¿qué se va a proteger? (activos de información y activos de apoyo); ¿quién lo va a proteger? (responsables, encargados o custodios); ¿cuál es la razón y la acción? (tratamiento o acción), ¿cuál es el periodo? (periodo de conservación).

[12] Para lograr que el SGSDP, sea parte del Partido de la Revolución Democrática, fue necesario: a) Comunicarlo a todos los involucrados; b) definir roles y responsabilidades; y c) puntualizar contribuciones y consecuencias de incumplimiento. Se recomienda que servidores partidistas, con cargos o funciones equiparables a una subdirección en la Administración Pública Federal u organismos constitucionalmente autónomos, tengan bajo su responsabilidad llevar a cabo la <<Política de Protección de Datos>> mismas que pueden formalizare a un mayor grado de pormenorización mediante <<mecanismos de rendición de cuentas>>.

[13] Al elaborar el Inventario de Datos Personales, se debe tomar en cuenta lo siguiente: a) Riesgo inherente en los sistemas de tratamiento; y b) aludir a las categorías de datos personales, p.e., especiales (que por su naturaleza y contexto pueden causar daño directo a los titulares), sensibles, o estándar. Deben contener, además: a) Catálogo de medios físicos y electrónicos y sus facultades; b) Catálogo de los tipos de datos personales que se traten; c) Catálogo de formatos de almacenamiento; d) Servidores partidistas que tienen acceso a los sistemas de tratamiento; e) Nombre completo o denominación o RFC del encargado y el instrumento jurídico; y f) Destinatario o terceros receptores de las transferencias.

[14] Para realizar el Análisis de Riesgo de los Datos Personales, se debe tomar en cuenta los factores para determinar las medidas de seguridad, que permiten definir los criterios de Evaluación del Riesgo, p.e., criterio de impacto (no contar con medidas de seguridad óptimas en sus sistemas de tratamiento para datos sensibles); criterio de aceptación (no tener un Aviso de Privacidad correcto).

*Activos; 2. Identificar Amenazas (una amenaza tiene potencial de dañar un activo, puede ser de origen natural o humano, accidentales o deliberadas y, además provenir de adentro o fuera de la organización, p.e. fuego o virus); 3. Identificar Vulnerabilidades (las vulnerabilidades son debilidades en los activos -material susceptible al fuego o la falta de un antivirus informáticos); y 4. Identificar Escenarios de Vulneración (es posible realizarlo mediante una matriz, cuyos principales indicadores sean: "**activo**", "**amenaza**", "**vulnerabilidad**", "**daño/impacto**", o "**potencial/probabilidad**".*

f. Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.

Mediante el Análisis de Brecha, es posible identificar: a) Las medidas de seguridad existentes; b) Las medidas de seguridad existentes que operan correctamente; c) Las medidas de seguridad faltantes; d) Si existen nuevas medidas de seguridad que puedan reemplazar a uno o más controles implementados actualmente.

b) Fase 2. Implementar el SGSDP:

a. Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales;

Las medidas de seguridad pueden ser, en un primer momento, físicas y ambientales; tecnológicas; controles de acceso al inmueble, o checadores que requieran datos biométricos como la huella digital.

Es importante plantear las siguientes preguntas: ¿qué dominios o controles ya tiene cubiertos un sujeto obligado?, o bien, ¿qué dominios podrían ayudar a mitigar los escenarios de riesgo identificados? Los controles con que se cuenta pueden contar con mayor o menor grado de madurez, dependiendo de si se encuentra en alguna de las siguientes posibles fases, estar: 1. Documentados; 2. Implementados; 3. Registrados; 4. Monitoreados; 5. Focalizados a identificadores clave de rendimiento; 6 En mejora continua; y 7. Automatizados.

Es evidente que un Sistema de Gestión de Protección de Datos, debe ser aplicado de manera cotidiana (situación que órganos intrapartidarios que remitieron insumos para este informe manifiestan cumplir), además de contar con un Plan de trabajo para la implementación de las medidas de seguridad faltantes, en ese sentido, el Departamento de Recursos Humanos e Informática del Partido de la Revolución Democrática manifestó que no ha sido puesto en conocimiento de vulneraciones a dispositivo electrónico alguno al seno del PRD, no obstante, periódicamente evalúa mejoras para garantizar que no se actualicen en el futuro dichas vulneraciones.

Lo anterior, es precisamente una manifestación que conduce a esta Unidad de Transparencia que el Plan de Trabajo para la implementación de las Medidas de Seguridad Faltantes es una actividad cotidiana en la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática.

Es vital puntualizar, como buena práctica, la siguiente metodología para su implementación en todo órgano intrapartidario para estar en posibilidades de cumplir con las medidas de seguridad para la protección de datos personales:

- *Cumplir con la política día a día: Un ejemplo claro, es señalar día con día a los empleados que no presentan credencial para accesar a la sede de algún órgano intrapartidario, que lo hagan.*
- *Aprobación de procedimientos donde se traten datos personales;*
- *Actualizaciones normativas respecto al tratamiento de datos personales; y*
- *Revisar que el Sistema de Gestión de Seguridad de Datos.*

c) Fase 3. Monitorear y Revisar el SGDP:

a. Paso 8. Revisiones y Auditoría.

¿Qué pasa si el Partido de la Revolución Democrática percibe un riesgo en el tratamiento de datos personales?

En primer lugar, debe notificar a las personas titulares de datos personales la vulneración para que esté en condiciones de tomar acciones de contención ante posibles daños patrimoniales, a su imagen o en cualquier otro aspecto, lo anterior, conforme al siguiente protocolo:

- *Reducir el riesgo: Implica la corrección; eliminación; prevención; minimización del impacto; disuasión; recuperación; monitoreo; y concientización. Para reducir un riesgo, p.e., se pueden emprender acciones como comprar antivirus, contar con reguladores de energía eléctrica, así como una política de respaldos de información.*
- *Retener el riesgo: No hay necesidad inmediata de implementar controles adicionales, no obstante, puede ser necesario ante el robo de bases de datos por alguna persona.*
- *Evitar el riesgo: Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios. Un ejemplo concreto, es evitar que los archivos estén cerca de las instalaciones sanitarias.*
- *Compartir el riesgo: Un tercero interviene para mitigar los posibles efectos de un riesgo.*
- *Aceptar el riesgo: Asumir formalmente las decisiones sobre el plan de tratamiento del riesgo.*
- *El resultado de lo anterior, nos conduce al <<riesgo residual>>*

Además de la revisión de factores de riesgo, los órganos intrapartidarios, en el marco de sus facultades y atribuciones, pueden realizar auditorías para prevenir, identificar y, en su caso, combatir vulneraciones a la seguridad de la información.

- *Acciones en caso de vulneración a la seguridad –*

1. *Identificación de la vulneración;*

2. *Notificación de la vulneración; y*

3. *Remediación del incidente.*

d) Fase 4. Mejorar el SGSDP:

a. Paso 9. Mejora Continua y Capacitación

Es importante generar escenarios prospectivos, prefentemente por los propios servidores partidistas del Partido de la Revolución Democrática, y así, estar en condiciones de realizar acciones preventivas y correctivas, al capacitar a dichos servidores partidistas, ha impulsado los ejes de concientización, entrenamiento y educación constante.

Amen de las políticas que se han establecido en términos de medidas de seguridad técnicas en materia de protección de datos personales, tales como asignación de contraseñas para correos electrónicos, equipos de cómputo u otras, se cuenta con privilegios para tener acceso a las bases de datos, en la mayoría de los casos de naturaleza administrativa (mediante oficio o contrato).

En la Décima Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática, órganos intrapartidarios remitieron pronunciamientos con la finalidad de colmar lo planteado en este punto y en el segundo trimestre del 2020, se emitirán oficios para aplicar la mejora continua al Documento de Seguridad del Partido de la Revolución Democrática, que siempre puede mejorar.

De los resultados de las evaluaciones para la generación de escenarios prospectivos, fue posible diseñar en plan de capacitación, que se encuentra alineado a los requerimientos de la Dirección General de Capacitación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como se podrá apreciar en los anexos del presente instrumento.

I. Programa General de Capacitación

Los Órganos Intrapartidarios, Unidad de Transparencia, Comité de Transparencia, así como la Dirección General de Capacitación, así como la Dirección General de Enlace con

Partidos Políticos y Organismos Descentralizados y Electorales del INAI, trabajamos en conjunto para que este Instituto político pudiera cumplir con los requisitos para ser distinguidos con las certificaciones de Institución y Comité de Transparencia 100% capacitados.

Durante el año 2019, conjuntamente con el Departamento de Recursos Humanos e Informática de la Coordinación de Patrimonio y Recursos Financieros del PRD, se notificó a todas las personas servidoras partidistas de este Instituto político para acudir a capacitaciones en los rubros de acceso a la información, transparencia, protección de datos, e incluso sobre gestión documental.

Posteriormente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Universidad Iberoamericana y el Partido de la Revolución Democrática, unieron esfuerzos para invitar a la Dra. Olivia Mendoza Enríquez[15]*, con la finalidad de que todo el personal del Partido de la Revolución Democrática Nacional, fuera capacitado en materia de protección de datos personales, capacitación que se realizó el día 4 de diciembre.*

Finalmente, el 16 de diciembre del 2019, el Titular de la Unidad de Transparencia del Partido de la Revolución Democrática, acudió a una invitación al Estado de Hidalgo para capacitar a los servidores partidistas de dicha entidad en materia Transparencia, Derecho de Acceso a la Información y Protección de Datos Personales.

No se omite mencionar que el programa de capacitación en materia de protección de datos personales, está alineado a la oferta académica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

II. Actualizaciones

El documento de seguridad, puede ser actualizado mediante los siguientes escenarios: a) cambios estructurales derivados de reformas a los documentos básicos o a los reglamentos del PRD; b) reformas a la Constitución Política de los Estados Unidos Mexicanos o a la normativa secundaria en materia de protección de datos personales; c) puesta en práctica de nuevos tratamientos de datos personales; y d) haber transcurrido un año desde la última actualización (únicamente para actualización de datos estadísticos).

III. Glosario de Términos

[15] https://www.youtube.com/watch?v=yT6pbbpdOL4&t=10s

Con la finalidad de ofrecer a la persona lectora, un glosario de términos que integre los principales conceptos en materia de transparencia, acceso a la información, protección de datos personales y gestión documental, me permito citar el artículo 3 del Reglamento de Transparencia, Acceso a la Información, Protección de Datos Personales y Gestión Documental del Partido de la Revolución Democrática:

*"**Artículo 3.** Para los efectos del presente reglamento, se entenderá por:*

***I. En materia de Transparencia y Acceso a la Información Pública**:*

a) ***Áreas:** Instancias que cuentan o puedan contar con la información, es decir, aquellas que estén previstas en el, Estatuto de este Instituto político;*

b) ***Comité de Transparencia:** Órgano colegiado al que hace referencia el artículo 64 de la Ley Federal de Transparencia y Acceso a la Información Pública;*

c) ***Consulta directa:** La prerrogativa que tiene toda persona para acceder a la información en la oficina habilitada para tal efecto;*

d) ***Datos abiertos:** Los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características: a) Accesibles: los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito; b) Integrales: contienen el tema que describen a detalle y con los metadatos necesarios; c) Gratuitos: se obtienen sin entregar a cambio contraprestación alguna; d) No discriminatorios: los datos están disponibles para cualquier persona, sin necesidad de registro; e) Oportunos: son actualizados, periódicamente, conforme se generen; f) Permanentes: se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto; g) Primarios: provienen de la fuente de origen con el máximo nivel de desagregación posible; h) Legibles por máquinas: deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática; i) En formatos abiertos: los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna; j) De libre uso: citan la fuente de origen, como único requerimiento para ser utilizados libremente;*

e) ***DDP:** Diccionario de Datos Personales;*

f) ***Documento**: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus servidores públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;*

g) ***Expediente:** Unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;*

h) ***Formatos abiertos:** Conjunto de características técnicas y de presentación de la información que corresponden a la estructura lógica usada para almacenar datos de forma integral y facilitan su procesamiento digital, cuyas especificaciones están disponibles públicamente y que permiten el acceso sin restricción de uso por parte de los usuarios;*

i) ***Formatos accesibles:** Cualquier manera o forma alternativa que dé acceso a los solicitantes de información, en forma tan viable y cómoda como la de las personas sin discapacidad ni otras dificultades para acceder a cualquier texto impreso y/o cualquier otro formato convencional en el que la información pueda encontrarse;*

j) ***Información de interés público:*** *Se refiere a la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados;*

k) ***INAI:*** *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;*

l) ***LPIASAI:*** *Lineamientos que establecen los Procedimientos Internos de Atención a Solicitudes de Acceso a la Información Pública;*

m) ***LFTAIP:*** *Ley Federal de Transparencia y Acceso a la Información Pública;*

n) ***LGTAIP:*** *Ley General de Transparencia y Acceso a la Información Pública;*

o) ***LGMCDIEVP:*** *Lineamientos Generales en Materia de Clasificación y Descalificación de la Información, así como para la elaboración de las Versiones Públicas;*

p) ***Lineamientos Técnicos Generales:*** *Lineamientos Técnicos Generales para la Publicación, Homologación y Estandarización de la Información de las Obligaciones Establecidas en el Título Quinto y en la Fracción IV del Artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben difundir los Sujetos Obligados en los Portales de Internet y en la Plataforma Nacional de Transparencia;*

q) ***Publicación:*** *La divulgación, difusión y socialización de la información por cualquier medio, incluidos los impresos, electrónicos, sonoros y visuales;*

r) ***Unidad de Transparencia:*** *Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública; y,*

s) ***Versión Pública:*** *Documento o expediente en el que se da acceso a información, eliminando u omitiendo las partes o secciones clasificadas.*

II. En materia de Protección de Datos Personales, se entenderá por:

a) ***Aviso de privacidad:*** *Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;*

b) ***Bases de datos:*** *Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;*

c) ***Bloqueo:*** *La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;*

d) ***Comité de Transparencia:*** *Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;*

e) ***Cómputo en la nube:*** *Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;*

f) ***Consentimiento:*** *Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;*

g) ***Datos personales:*** *Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;*

h) ***Datos personales sensibles:*** *Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales*

que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

i) ***Derechos ARCO:*** *Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;*

j) ***Disociación:*** *el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;*

k) ***Documento de seguridad:*** *Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;*

l) ***Encargado:*** *La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;*

m) ***Evaluación de impacto en la protección de datos personales:*** *Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;*

n) ***Fuentes de acceso público:*** *Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;*

o) ***Medidas compensatorias:*** *Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;*

p) ***Medidas de seguridad:*** *Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;*

q) ***Medidas de seguridad administrativas:*** *Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;*

r) ***Medidas de seguridad físicas:*** *Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro del Partido, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;*

s) ***Medidas de seguridad técnicas:*** *Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de*

seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

t) ***LGPDP:*** *Lineamientos Generales de Protección de Datos Personales;*

u) ***LGPDPPSO:*** *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;*

v) ***Remisión:*** *Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;*

w) ***Responsable:*** *Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;*

x) ***Sistema Nacional:*** *El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;*

y) ***Supresión:*** *La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;*

z) ***Titular:*** *La persona física a quien corresponden los datos personales;*

aa) ***Transferencia:*** *Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado; y,*

bb) ***Tratamiento:*** *Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.*

III. En materia de gestión documental y archivos, se entenderá por:

a) ***Acervo:*** *El conjunto de documentos producidos y recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones con independencia del soporte, espacio o lugar que se resguarden;*

b) ***Actividad archivística:*** *El conjunto de acciones encaminadas a administrar, organizar, conservar y difundir documentos de archivo;*

c) ***Archivo:*** *El conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden;*

d) ***Archivo de concentración:*** *El integrado por documentos transferidos desde las áreas o unidades productoras, cuyo uso y consulta es esporádica y que permanecen en él hasta su disposición documental;*

e) ***Archivo de trámite:*** *El integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados;*

f) ***Archivo General:*** *El Archivo General de la Nación;*

g) ***Archivos generales:*** *Las entidades especializadas en materia de archivos en el orden local, que tienen por objeto promover la administración homogénea de los archivos, preservar, incrementar y difundir el patrimonio documental de la entidad federativa, con el fin de salvaguardar su memoria de corto, mediano y largo plazo, así como contribuir a la transparencia y rendición de cuentas;*

h) ***Archivo histórico:*** *El integrado por documentos de conservación permanente y de relevancia para la memoria nacional, regional o local de carácter público;*

i) ***Archivos privados de interés público:*** *El conjunto de documentos de interés público, histórico o cultural, que se encuentran en propiedad de particulares, que no reciban o ejerzan recursos públicos ni realicen actos de autoridad en los diversos ámbitos de gobierno;*

j) ***Área coordinadora de archivos:*** *La instancia encargada de promover y vigilar el cumplimiento de las disposiciones en materia de gestión documental y administración de archivos, así como de coordinar las áreas operativas del sistema institucional de archivos;*

k) ***Áreas operativas:*** *Las que integran el sistema institucional de archivos, las cuales son la unidad de correspondencia, archivo de trámite, archivo de concentración y, en su caso, histórico;*

l) ***Baja documental:*** *La eliminación de aquella documentación que haya prescrito su vigencia, valores documentales y, en su caso, plazos de conservación; y que no posea valores históricos, de acuerdo con la Ley y las disposiciones jurídicas aplicables;*

m) ***Catálogo de disposición documental:*** *Al registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental;*

n) ***Ciclo vital:*** *Las etapas por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico;*

o) ***Consejos Locales:*** *Los consejos de archivos de las entidades federativas;*

p) ***Conservación de archivos:*** *El conjunto de procedimientos y medidas destinados a asegurar la prevención de alteraciones físicas de los documentos en papel y la preservación de los documentos digitales a largo plazo;*

q) ***Consulta de documentos:*** *Las actividades relacionadas con la implantación de controles de acceso a los documentos debidamente organizados que garantizan el derecho que tienen los usuarios mediante la atención de requerimientos;*

r) ***Cuadro general de clasificación archivística:*** *Al instrumento técnico que refleja la estructura de un archivo con base en las atribuciones y funciones de cada sujeto obligado;*

s) ***Datos abiertos:*** *Los datos digitales de carácter público que son accesibles en línea y pueden ser usados, reutilizados y redistribuidos, por cualquier interesado;*

t) ***Disposición documental:*** *La selección sistemática de los expedientes de los archivos de trámite o concentración cuya vigencia documental o uso ha prescrito, con el fin de realizar transferencias ordenadas o bajas documentales;*

u) ***Documento de archivo:*** *Aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental;*

v) ***Documentos históricos:*** *Los que se preservan permanentemente porque poseen valores evidénciales, testimoniales e informativos relevantes para la sociedad, y que por ello forman parte íntegra de la memoria colectiva del país y son fundamentales para el conocimiento de la historia nacional, regional o local;*

w) ***Estabilización:*** *El procedimiento de limpieza de documentos, fumigación, integración de refuerzos, extracción de materiales que oxidan y deterioran el papel y resguardo de documentos sueltos en papel libre de ácido, entre otros;*

x) ***Expediente:*** *La unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;*

y) ***Expediente electrónico:*** *El conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan;*

z) ***Ficha técnica de valoración documental:*** *El instrumento que permite identificar, analizar y establecer el contexto y valoración de la serie documental;*

aa) ***Firma electrónica avanzada:*** *El conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;*

bb) ***Fondo:*** *El conjunto de documentos producidos orgánicamente por un sujeto obligado que se identifica con el nombre de este último;*

cc) ***Gestión documental:*** *Al tratamiento integral de la documentación a lo largo de su ciclo vital, a través de la ejecución de procesos de producción, organización, acceso, consulta, valoración documental y conservación;*

dd) ***Grupo interdisciplinario:*** *Al conjunto de personas que deberá estar integrado por el titular del área coordinadora de archivos; la unidad de transparencia; los titulares de las áreas de planeación estratégica, jurídica, mejora continua, órganos internos de control o sus*

equivalentes; las áreas responsables de la información, así como el responsable del archivo histórico, con la finalidad de coadyuvar en la valoración documental;

ee) ***Interoperabilidad:*** *La capacidad de los sistemas de información de compartir datos y posibilitar el intercambio entre ellos;*

ff) ***Instrumentos de control archivístico:*** *Los instrumentos técnicos que propician la organización, control y conservación de los documentos de archivo a lo largo de su ciclo vital que son el cuadro general de clasificación archivística y el catálogo de disposición documental;*

gg) ***Instrumentos de consulta:*** *Los instrumentos que describen las series, expedientes o documentos de archivo y que permiten la localización, transferencia o baja documental;*

hh) ***Inventarios documentales:*** *Los instrumentos de consulta que describen las series documentales y expedientes de un archivo y que permiten su localización (inventario general), para las transferencias (inventario de transferencia) o para la baja documental (inventario de baja documental);*

ii) ***Metadatos:*** *El conjunto de datos que describen el contexto, contenido y estructura de los documentos de archivos y su administración, a través del tiempo, y que sirven para identificarlos, facilitar su búsqueda, administración y control de acceso;*

jj) ***Organización:*** *El conjunto de operaciones intelectuales y mecánicas destinadas a la clasificación, ordenación y descripción de los distintos grupos documentales con el propósito de consultar y recuperar, eficaz y oportunamente, la información. Las operaciones intelectuales consisten en identificar y analizar los tipos de documentos, su procedencia, origen funcional y contenido, en tanto que las operaciones mecánicas son aquellas actividades que se desarrollan para la ubicación física de los expedientes;*

kk) ***Patrimonio documental:*** *Los documentos que, por su naturaleza, no son sustituibles y dan cuenta de la evolución del Estado y de las personas e instituciones que han contribuido en su desarrollo; además de transmitir y heredar información significativa de la vida intelectual, social, política, económica, cultural y artística de una comunidad, incluyendo aquellos que hayan pertenecido o pertenezcan a los archivos de los órganos federales, entidades federativas, municipios, alcaldías de la Ciudad de México, casas culturales o cualquier otra organización, sea religiosa o civil;*

ll) ***Plazo de conservación:*** *El periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.*

mm) ***Programa anual:*** *El Programa anual de desarrollo archivístico;*

nn) ***Sección:*** *Cada una de las divisiones del fondo documental basada en las atribuciones de cada sujeto obligado de conformidad con las disposiciones legales aplicables;*

oo) ***Serie:*** *La división de una sección que corresponde al conjunto de documentos producidos en el desarrollo de una misma atribución general integrados en expedientes de acuerdo a un asunto, actividad o trámite específico;*

pp) ***Sistema Institucional:*** *A los sistemas institucionales de archivos de cada sujeto obligado;*

qq) ***Sistema Local:*** *Los sistemas de archivos en las entidades federativas; LIII. Sistema Nacional: Al Sistema Nacional de Archivos;*

rr) ***Soportes documentales:*** *Los medios en los cuales se contiene información además del papel, siendo estos materiales audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros, visuales, entre otros.*

ss) ***Subserie:*** *La división de la serie documental;*

tt) ***Transferencia:*** *El traslado controlado y sistemático de expedientes de consulta esporádica de un archivo de trámite a uno de concentración y de expedientes que deben conservarse de manera permanente, del archivo de concentración al archivo histórico;*

uu) ***Trazabilidad:*** *La cualidad que permite, a través de un sistema automatizado para la gestión documental y administración de archivos, identificar el acceso y la modificación de documentos electrónicos.*

vv) ***Valoración documental:*** *La actividad que consiste en el análisis e identificación de los valores documentales; es decir, el estudio de la condición de los documentos que les confiere características específicas en los archivos de trámite o concentración, o evidénciales, testimoniales e informativos para los documentos históricos, con la finalidad de establecer criterios, vigencias documentales y, en su caso, plazos de conservación, así como para la disposición documental; y,*

ww) ***Vigencia documental:*** *El periodo durante el cual un documento de archivo mantiene sus valores administrativos, legales, fiscales o contables, de conformidad con las disposiciones jurídicas vigentes y aplicables."*

Ahora bien, también se precisan los siguientes términos:

1. ***Activos:*** *Cualquier recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización: activos de información (son los datos personales); y activos de apoyo (p.e. cuando estos son recabados mediante formularios impresos).*

2. ***Alta Dirección:*** *Toda persona con poder legal de toma de decisiones en las políticas de la organización.*

3. ***Confidencialidad:*** *Propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas. Se busca prevenir la divulgación no autorizada de información.*

4. ***CT-PRD:*** *Comité de Transparencia del Partido de la Revolución Democrática;*

5. ***Custodio:*** *Toda persona con responsabilidad funcionar sobre los activos.*

6. ***Disponibilidad.*** *Propiedad de un activo para ser accesible y utilizable Permite controlar las interrupciones de los recursos; y prevenir interrupciones no autorizadas. En síntesis, permite contar con información exacta y completa, para ser revelada, accesible y utilizable sólo para las personas autorizadas.*

   Para efectos de esta definición, por integridad se entiende que la información sea la correcta, por confidencialidad que sea destinada a la persona correcta y, por disponibilidad que esto se lleve a cabo en el momento correcto.

7. ***DRHI-CPRF-PRD:*** *Departamento de Recursos Humanos e Informática del Partido de la Revolución Democrática;*

8. ***Estatuto del Partido de la Revolución Democrática vigente:*** *Estatuto del Partido de la Revolución Democrática aprobado en el XV Congreso Nacional Extraordinario, celebrado los días 17 y 18 de noviembre de 2018 (DOF: 28-12-2018)*[16]*; y el Estatuto del Partido de la Revolución Democrática aprobado en el XVI Congreso Nacional Extraordinario, celebrado*

16 https://www.dof.gob.mx/nota_detalle.php?codigo=5547433&fecha=28/12/2018&print=true

los días 31 de agosto y 1 de septiembre de 2019 (DOF: 22-11-2019)[17];

9. ***Integridad:*** *Es la propiedad de salvaguardar la exactitud y la completitud de los activos. Evitar la modificación no autorizada o accidental.*

10. ***Instituto político:*** *Partido de la Revolución Democrática;*

11. ***LGPDPPSO:*** *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados;*

1. ***Normativa intrapartidaria:*** *Documentos básicos y reglamentos del Partido de la Revolución Democrática registrados ante la Dirección Ejecutiva de Prerrogativas y Partidos Políticos del Instituto Nacional Electoral, a saber: Estatuto del Partido de la Revolución Democrática aprobado en el XV Congreso Nacional Extraordinario, celebrado los días 17 y 18 de noviembre de 2018 (DOF: 28-12-2018)[18]; Congreso Nacional Extraordinario, celebrado los días 31 de agosto y 1 de septiembre de 2019 (DOF: 22-11-2019)[19]; Declaración de Principios; Programa de Acción; Reglamento del Congreso Nacional; Reglamento de las Coordinadoras de Autoridades Locales; Reglamento de Transparencia, Acceso a la Información, Protección de Datos Personales y Gestión Documental; Reglamento de Afiliación; Reglamento de los Consejos; Reglamento de Direcciones; Reglamento de Elecciones; Reglamento de las Direcciones de Comunicación Nacional y Estatales; Reglamento del Instituto de Formación Política; Reglamento de la Organización Nacional de Mujeres; Reglamento del Órgano de Justicia Intrapartidaria; Reglamento del Patrimonio y Recursos Financieros; Reglamentos de Organización Nacional de Juventudes de Izquierda del Partido de la Revolución Democrática; y el Reglamento del Instituto de Formación Política, todos ellos, del Partido de la Revolución Democrática.*

12. ***Partido político:*** *Partido de la Revolución Democrática;*

13. ***PRD:*** *Partido de la Revolución Democrática;*

14. ***Seguridad de la Información****: Se busca evitar modificaciones no autorizadas o accidentales; evitar acceso o divulgación no autorizados; que los activos se puedan utilizar por los autorizados, cuando se requiere; en suma, preservar la confidencialidad, integridad y disponibilidad de los activos.*

15. ***Sistema de Gestión de Datos Personales****: Es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.*

16. ***UT-PRD:*** *Unidad de Transparencia del Partido de la Revolución Democrática;*

IV. Aprobación de Documento de Seguridad

17 https://www.dof.gob.mx/nota_detalle.php?codigo=5579643&fecha=22/11/2019

18 https://www.dof.gob.mx/nota_detalle.php?codigo=5547433&fecha=28/12/2018&print=true

19 https://www.dof.gob.mx/nota_detalle.php?codigo=5579643&fecha=22/11/2019

La aprobación del Documento de Seguridad del Partido de la Revolución Democrática se realizó con reservas mediante la Segunda Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática celebrada el diecisiete de febrero del año dos mil veinte, se aprobó el Dictamen del Documento de Seguridad del Partido de la Revolución Democrática 2019, como se puede observar mediante el siguiente hipervínculo, https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2020/2S_Ordinaria_17-02-20.pdf, así como en la Segunda Sesión Ordinaria del Comité de Transparencia del Partido de la Revolución Democrática celebrada el diecisiete de febrero del año dos mil veinte, se aprobó el Dictamen del Documento de Seguridad del Partido de la Revolución Democrática 2019, como se puede observar mediante el siguiente hipervínculo, https://transparencia-prd.org.mx/documentos/art_70/fracc_XXXIX/2020/2S_Ordinaria_17-02-20.pdf"

CONSIDERANDOS

PRIMERO.- El Comité de Transparencia del Partido de la Revolución Democrática es competente para autorizar el *Documento de Seguridad del Partido de la Revolución Democrática*, en los términos del artículo 35 y 84 de la *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, así como de los artículos 123 a 135* del *Estatuto del Partido de la Revolución Democrática* aprobado en el XV Congreso Nacional Extraordinario, celebrado los días 17 y 18 de noviembre de 2018 (DOF: 28-12-2018)[20]; y los artículos 128 al 138 del *Estatuto del Partido de la Revolución Democrática aprobado en el XVI Congreso Nacional Extraordinario, celebrado los días 31 de agosto y 1 de septiembre de* 2019 (DOF: 22-11-2019)[21]

SEGUNDO.- Este Comité de Transparencia fundamenta su actuar con base en la *Declaración Universal de Derechos Humanos*; *Convención Interamericana de Derechos Humanos*; *el CONVENIO N° 108 DEL CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL Y PROTOCOLO*

20 https://www.dof.gob.mx/nota_detalle.php?codigo=5547433&fecha=28/12/2018&print=true

21 https://www.dof.gob.mx/nota_detalle.php?codigo=5579643&fecha=22/11/2019

ADICIONAL AL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, A LAS AUTORIDADES DE CONTROL Y A LOS FLUJOS TRASFRONTERIZOS DE DATOS; *PROTOCOLO ADICIONAL AL CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, A LAS AUTORIDADES DE CONTROL Y A LOS FLUJOS TRANSFRONTERIZADOS DE DATOS* (Estrasburgo, 8.XI.2001[22]); el *Tratado Comercial entre México Estados Unidos y Canadá* (TEMEC); la *Constitución Política de los Estados Unidos Mexicanos*; la *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados* (Art. 35); y los artículos 128 al 135 del *Estatuto del Partido de la Revolución Democrática* aprobado en el XV Congreso Nacional Extraordinario, celebrado los días 17 y 18 de noviembre de 2018 (DOF: 28-12-2018)[23]; y los artículos 128 al 138 del *Estatuto del Partido de la Revolución Democrática aprobado en el XVI Congreso Nacional Extraordinario, celebrado los días 31 de agosto y 1 de septiembre de* 2019 (DOF: 22-11-2019)[24]. Todo lo anterior, en aras de hacer valer en favor de la sociedad, de manera efectiva, el principio pro persona, consagrado en el artículo 1° de la *Constitución Política de los Estados Unidos Mexicanos*.

TERCERO.- La Unidad de Transparencia refiere en el *Capítulo de Medidas de Seguridad*, que diversos órganos intrapartidarios coinciden en cuanto a las medidas de seguridad físicas y administrativas, según lo valorado en la *DÉCIMA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA* (celebrada en 2019). También plantea un esquema metodológico del *Sistema de Gestión de Protección de Datos Personales* del Partido de

---

[22] Apenas un año después de la creación del otrora IFAI.

[23] https://www.dof.gob.mx/nota_detalle.php?codigo=5547433&fecha=28/12/2018&print=true

[24] https://www.dof.gob.mx/nota_detalle.php?codigo=5579643&fecha=22/11/2019

la Revolución Democrática. Finalmente, en el capítulo intitulado *ACTUALIZACIONES*, hace referencia a distintos escenarios que deben dar pie a una actualización del documento que nos ocupa. Por lo anterior, es importante que la Unidad de Transparencia, perfeccione el *Informe del Documento de Seguridad* que nos ocupa, en los siguientes términos:

- En cuanto hace a las medidas de seguridad, este Comité de Transparencia considera que es necesario que se giren oficios a los órganos intrapartidarios del PRD, para que aporten elementos que permitan dotar de mayor precisión el documento de marras que permitan una mejor integración del *Documento de Seguridad del Partido de la Revolución Democrática*, en futuras sesiones que tengan por objeto la actualización del documento que nos ocupa.
- Con relación al Sistema de Gestión antes referido, es necesario que la Unidad de Transparencia, brinde una narrativa más pormenorizada a la sociedad, con la finalidad de exponenciar el cumplimiento material del derecho humano a la protección de datos personales.
- Finalmente, en cuanto a las causales de actualización del Documento de Seguridad, se instruye a la Unidad de Transparencia a incluir como causales de actualización, las referidas en el artículo 36 de la *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.*

De lo anteriormente referido, se desprende que la Unidad de Transparencia ha realizado un trabajo integrador de las manifestaciones que distintos órganos intrapartidarios han realizado para definir en el ámbito de sus facultades y atribuciones, los contenidos del Documento de Seguridad del PRD. No es óbice mencionar que, para garantizar el cumplimiento del principio de certeza jurídica, se convocó a cada órgano intrapartidario del PRD, para que se pronunciaran sobre los términos en que tratan datos personales. De lo anterior, es posible afirmar que la fase primordial en la integración del documento de seguridad que nos ocupa, es el trabajo conjunto entre órganos intrapartidarios, coordinados por la Unidad de Transparencia y el Comité de Transparencia del Partido de

la Revolución Democrática y, en un acto posterior, se procede a integrar todas las manifestaciones y pronunciamientos para ofrecer a la sociedad el instrumento intitulado: *"DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA".*

Es evidente, que la obligación de este Instituto Político con relación a contar con un documento de seguridad que resulte comprensible para las personas que lo consulten, se traduce en una necesidad inminente, pues se trata de una obligación jurídica expresa contenida en el artículo 35 de la *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados*, sirve como respaldo a lo anterior la siguiente tesis aislada:

"Tesis: X.3o.16 P	*Semanario Judicial de la Federación y su Gaceta*	*Novena Época*	*194501 3 de 5*
Tribunales Colegiados de Circuito	*Tomo IX, Marzo de 1999*	*Pag. 1374*	*Tesis Aislada(Penal)*

ACTOS RECLAMADOS INMINENTES. LO SON AQUELLOS DE CUYA REALIZACIÓN SE TIENE PLENA CERTEZA POR SER UNA CONSECUENCIA FORZOSA E INELUDIBLE DE HECHOS PROBADOS.

La resolución dictada por la Sala Penal del Tribunal Superior de Justicia del Estado, que revoca el auto que negó la orden de aprehensión y detención en contra del quejoso por el delito de incumplimiento de las obligaciones de asistencia familiar cometido en agravio de su cónyuge y menores hijos, por estimar que en la especie se acreditan los elementos del tipo penal, así como la presunta responsabilidad del inconforme, produce en el quejoso un agravio actual, pues si bien la resolución reclamada, por sí sola, no afecta la libertad del quejoso, también es cierto que por referirse a una situación que está pronta a suceder, como lo es la orden de aprehensión, seguramente se lo causará; esto es así, a virtud de que si la autoridad ordenadora consideró que en el caso con los elementos de prueba se

*acreditan tanto los elementos del tipo del delito de incumplimiento de las obligaciones de asistencia familiar, cuanto la probable responsabilidad del quejoso, es evidente que dicha resolución obliga al Juez responsable a emitir la orden de aprehensión en contra del impetrante por el referido ilícito, porque ese tipo de mandamiento judicial ya no depende del análisis y valoración de las pruebas de autos por parte del Juez, quien ha de dictarla, pues no obstante de que la Sala Penal dejó plenitud de jurisdicción al Juez natural, enseguida precisó que debía dictar otra de acuerdo a los lineamientos de la resolución de segunda instancia; por tanto, se trata de un acto de realización inminente, por ser una consecuencia forzosa e ineludible de **hechos** probados respecto del cual es procedente el juicio de amparo biinstancial. Estimar lo contrario implicaría que aunque el gobernado tuviera pleno conocimiento de la realización próxima de un acto lesivo, para intentar el amparo estaría obligado a esperar la realización de dicho acto, con todas las consecuencias perjudiciales que ello acarrea, so pena de que se sobreseyera en el juicio promovido con anticipación a dicho evento, lo que es contrario a la naturaleza del juicio de amparo.*

TERCER TRIBUNAL COLEGIADO DEL DÉCIMO CIRCUITO.

Amparo en revisión 568/98. Marco Antonio Vivanco Mendoza. 15 de enero de 1999. Unanimidad de votos. Ponente: César Thomé González. Secretaria: Fidelia Camacho Rivera.
Véase: Semanario Judicial de la Federación, Octava Época, Tomo I, Segunda Parte-1, página 56, tesis de rubro: "ACTOS RECLAMADOS. NATURALEZA JURÍDICA DE LOS ACTOS INMINENTES, EN SU POSICIÓN FRENTE A LOS ACTOS YA EXISTENTES Y A LOS FUTUROS.".

De lo anterior se colige que, pese a que existieran áreas de oportunidad en la integración del *Documento de Seguridad* que nos ocupa, este Comité de Transparencia, está obligado a aprobar, con reservas, dicho instrumento, **sin que las responsabilidades inherentes le puedan ser imputables, pues como ha sido debidamente expuesto, se actúa en pro**

del derecho humano de protección de datos personales de la sociedad, y las actuaciones que corresponden a cada órgano intrapartidario han sido valoradas para poder determinar las razones por las cuales el documento debe ser aprobado con reservas.

Por lo anterior, este Comité de Transparencia propone resolver:

PRIMERO.- Aprobar con las reservas establecidas en el *TERCER CONSIDERANDO*, el *Documento de Seguridad en materia de Protección de Datos Personales del Partido de la Revolución Democrática*, en aras de salvaguardar el cumplimiento material del derecho humano a la protección de datos personales en pro de la sociedad, **advirtiendo desde este momento, las acciones necesarias para que dicho documento, de darse las condiciones, pueda ser aprobado sin reserva alguna.**

SEGUNDO.- Ordenar a la Unidad de Transparencia que gire los oficios necesarios para perfeccionar el *Documento de Seguridad en materia de Protección de Datos Personales del Partido de la Revolución Democrática* y, a la brevedad posible, haga del conocimiento del Departamento Jurídico de la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática, en el ámbito de sus facultades y atribuciones, lo conducente.

TERCERO.- Instruir a la Unidad de Transparencia del Partido de la Revolución Democrática a que, una vez cumplido lo dispuesto en el resolutivo *SEGUNDO*, presente de nueva cuenta a este Comité de Transparencia un proyecto de *Documento de Seguridad en materia de Protección de Datos Personales del Partido de la Revolución Democrática*, que atienda plenamente a las áreas de oportunidad que han sido descritas en este

instrumento, previa valoración del Departamento Jurídico de la Coordinación de Patrimonio y Recursos Financieros del Partido de la Revolución Democrática.

CUARTO.- Instruir a la Unidad de Transparencia de este Instituto político que, previo a la publicación del *Documento de Seguridad en materia de Protección de Datos Personales del Partido de la Revolución Democrática*, en el Portal de este Instituto Político, con las reservas antes referidas, añada las causales de actualización de dicho documento referidas en el artículo 36 de la *Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.*

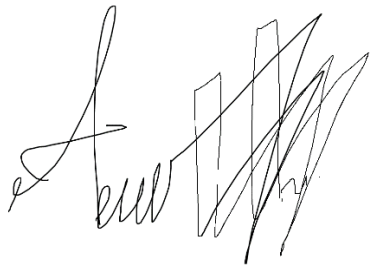
Por todo lo anterior, se solicita al Pleno de este Comité de Transparencia que, en caso de estar de acuerdo con el proyecto de resolución del *TERCER PUNTO* del *ORDEN DEL DÍA*, se sirvan manifestarlo con votación económica.

Al computarse dos votos a favor, con fundamento en los artículos 1°, 6°, 16, párrafo segundo de la *Constitución Política de los Estados Unidos Mexicanos*, así como lo dispuesto en el primer *CONSIDERANDO*.

En el uso de la palabra el C. Antonio Aarón Ávalos de Anda, en su calidad de Presidente del Comité de Transparencia, manifestó: "Integrantes del Comité de Transparencia, toda vez que, con fecha dieciséis de abril de dos mil veinte, en los términos planteados, se ha agotado el tercer punto del orden del día, se tiene como último punto a tratar el marcado con el número **4**, consistente en "*clausura*", agradeciendo mucho su presencia y siendo las DIECIOCHO HORAS CON TREINTA MINUTOS, del día 16 de abril de 2020, se da por concluida la Cuarta Sesión Extraordinaria del Comité de Transparencia del Partido de la Revolución Democrática, en esta anualidad. -

La presente acta consta de 75 fojas útiles por un solo lado anverso, incluyendo la hoja de firmas, cada una firmada al margen y al calce por los Integrantes del Comité de Transparencia del Partido de la Revolución Democrática. -

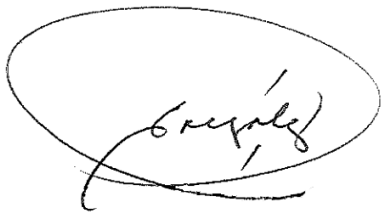
Estas firmas pertenecen al ACTA DE LA CUARTA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA, en esta anualidad.



C. Representante de la Dirección Nacional Extraordinaria
Integrante del Comité de Transparencia del Partido de la Revolución Democrática

Mtro. Antonio Aarón Avalos de Anda

Presidente del Comité de Transparencia del Partido de la Revolución Democrática



Lic. Salvador González García
Integrante del Comité de Transparencia del Partido de la Revolución Democrática