

Prospectivas de Implementación Tecnológica en la Administración Pública: México

PRODECON



**Procuraduría
de la Defensa
del Contribuyente**
PROTEGE • DEFIENDE • OBSERVA

Prospectivas de Implementación Tecnológica en la
Administración Pública: México

PRODECON

CUADERNOS INSTITUCIONALES



D.R. © PROCURADURÍA DE LA DEFENSA DEL CONTRIBUYENTE

Insurgentes Sur 954, Colonia Insurgentes San Borja, Alcaldía Benito Juárez
C.P. 03100, México, CDMX.

Teléfonos: (55) 1205-9000, 800 611 0190
www.prodecon.gob.mx

Septiembre 2020

***Con especial dedicatoria a todas aquellas personas que
por COVID-19 ya no se encuentran en este mundo....***

Prospectivas de Implementación Tecnológica en la Administración Pública: México

PRODECON

Índice

Introducción	5
Sociedad Digital	8
Adaptación Digital, caso PRODECON	14
Contrastando Derechos Digitales	39
Neutralidad en la red	43
Acceso a internet	46
Ciberseguridad	48
Protección a menores en las TIC	54
Sobre los datos personales	57
Intimidad y desconexión laboral	61
Políticas de impulso a Derechos Digitales	62
Futuros usos tecnológicos	65
Consideraciones Finales	71
Bibliografía	73

Introducción



La sociedad mexicana está atravesando un completo desafío, incluso extendido y solidarizado de manera global, un punto de adaptación, creación, implementación con miras hacia un contexto distinto a lo acostumbrado. Y es que, ante los nuevos retos que se enfrentan a nivel global, a poco tiempo de haber comenzado el año 2020, la llegada del COVID-19 en el primer trimestre fue inminente, ante una expansión global del nuevo virus que aqueja a la humanidad y ha puesto en jaque a naciones enteras, el comenzar a migrar casi obligadamente hacia un plano intangible, es decir, hacia lo digital, ha traído una serie de retos, que en el caso de México, requiere que hagamos un contraste entre el contenido de las políticas públicas y el desarrollo de la tutela de Derechos Digitales homologados a Derechos Humanos para los usuarios en México.

En este contexto, se reflexiona sobre el ejercicio particular de la Procuraduría de la Defensa del Contribuyente (**PRODECON**) y su apuesta por la implementación tecnológica para un correcto y mayor alcance de sus funciones, en defensa de los contribuyentes.

A partir de la premisa de que el mundo está en constante cambio, no debemos ser reacios al avance tecnológico, puesto que utilizar a las Tecnologías de la Información y de la Comunicación (TIC), en nuestras labores cotidianas, e incluso por ocio y necesidad, hace que la simplificación de tareas, (mismas que hasta hace algunas décadas hubiesen sido utópicas), sea una completa realidad.

Si bien, la tecnología crece día a día y para el derecho es casi imposible poder tutelar cada una de las nuevas conductas

derivadas del uso tecnológico, el conocer de un panorama actual y de vanguardia para buscar una correcta conjunción técnica/legal mejorará y potencializará el pensamiento digital de todo actor en el ámbito gubernamental.

Ahora bien, en este momento sabemos que el SARS-CoV-2, también conocido como Covid-19, es un virus que apareció en China y después se extendió a todos los continentes del mundo provocando una pandemia siendo Europa y América los más afectados¹.

Ante el esparcimiento del virus, cada nación en el mundo optó por planes de contención y medidas sanitarias con la finalidad de lograr un resguardo poblacional y no llegar a una carencia de insumos, equipo y espacio en hospitales. En México se optó por llevar a cabo un periodo de aislamiento y mínima interacción entre la sociedad, a la par de refuerzos como el uso de cubrebocas, sana distancia, gel antibacterial, entre otros.

Para las dependencias y entidades gubernamentales se presentaron una serie de retos para poder continuar vía remota sus funciones, sobre todo las actividades presenciales acostumbradas, sin duda un completo desafío si analizamos e identificamos que hace falta mucha conciencia sobre temas digitales. En un primer momento, las herramientas técnicas como redes privadas virtuales o VPN's se convirtieron en el vínculo directo hacia los servidores y sistemas de cada una de las dependencias; sin embargo, no comienza todo desde la solución o herramienta implementada, sino con la concientización y sensibilización del funcionario público sobre el tema digital, con la intención de familiarizarse intrínsecamente con el buen funcionamiento, prácticas y adopción de un

.....
1. Gobierno de México. 2020. Información general. Recuperado de <https://coronavirus.gob.mx/informacion-accesible/>

esquema de teletrabajo, el cual resulta tener una función mayor al estereotipo planteado y relacionado con el “*home office*”.

Esto quiere decir que la necesidad de tener que dar una concientización sobre la forma en como dirigirse a otros usuarios en el ciberespacio, las reglas de convivencia digital, también conocidas como “*netiqueta*”, son el punto base, que se vuelve una prioridad, al dejar en claro que la forma de interactuar, en medios digitales y plataformas, tiene una serie de lineamientos para el funcionamiento y relaciones como entes digitales, conocidos como usuarios.

Para el caso pertinente de la Procuraduría de la Defensa del Contribuyente, a raíz del distanciamiento social generado con motivo de la pandemia, se llevaron talleres de capacitación en línea, acortando la distancia gracias a las TIC.

Y es que, internet se ha convertido en una de las herramientas más poderosas para la humanidad, ya que no conoce fronteras, acerca personas geográficamente separadas, lo que facilita y simplifica tareas; todos estos elementos son la esencia de las TIC. Para el desarrollo de nuestro tema es pertinente, desatacar que, internet se ha convertido en una herramienta poderosa para el ejercicio de los Derechos Humanos, bien reflejados en el ciberespacio y a través de la tecnología, los llamados Derechos Digitales, los que serán abordados más adelante.

Sociedad Digital

Actualmente, el plano tecnológico relacionado con los derechos de los usuarios, en esta etapa de aislamiento se relaciona con un par de sucesos que desde hace años tienen impacto y muchas personas desconocen. El primer hecho es el Día Mundial de las Telecomunicaciones que se celebra, cada año, el 17 de mayo desde 1969, para conmemorar la fundación de la Unión Internacional de Telecomunicaciones (UIT) y la firma del primer Convenio Telegráfico Internacional en 1865, mismo que fue instituido por la Conferencia de Plenipotenciarios de Málaga-Torremolinos en 1973.

El otro suceso importante, fue en noviembre de 2005, cuando se celebró la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en donde se solicitó a la Asamblea General de las Naciones Unidas que declarase el 17 de mayo como el, “Día Mundial de la Sociedad de la Información”, para destacar la importancia de las Tecnologías de la información y las comunicaciones (TIC).

En noviembre de 2006, la Conferencia de Plenipotenciarios de la UIT en Antalya (Turquía) celebró el “Día Mundial de las Telecomunicaciones y la Sociedad de la Información”, el 17 de mayo. En la Resolución 68 actualizada, se invita a los Estados Miembros y los Miembros de Sector a celebrar todos los años ese día, organizando programas nacionales apropiados con objeto de:

- Estimular la reflexión y el intercambio de ideas sobre el tema elegido por el Consejo de la UIT.
- Realizar debates sobre los diversos aspectos del tema con todos los miembros de la sociedad.

- Elaborar un Informe que recoja las deliberaciones nacionales sobre los diferentes aspectos del tema, que se remitirá a la UIT y al resto de los Miembros².

México celebra desde hace tiempo el 17 de mayo, con la temática de Día Mundial de Internet, de forma resumida a los títulos antes mencionados, en el contexto de cumplir con los Objetivos de Desarrollo Sostenible de Naciones Unidas, con miras de la agenda 2030, pues en éstos se identifica un punto de convergencia y transversalidad entre la implementación tecnológica y el crecimiento.

Los Objetivos de Desarrollo Sostenible son el plan maestro para conseguir un futuro hacedero para todos. Se interrelacionan entre sí e incorporan los desafíos globales a los que nos enfrentamos día a día, como la pobreza, la desigualdad, el clima, la degradación ambiental, la prosperidad, la paz y la justicia, los mismos que deben alcanzarse para 2030 y que a continuación se enuncian:

- 1.- Erradicar la pobreza en todas sus formas en todo el mundo.
- 2.- Poner fin al hambre, conseguir la seguridad alimentaria y una mejor nutrición, y promover la agricultura sostenible.
- 3.- Garantizar una vida saludable y promover el bienestar para todos para todas las edades.
- 4.- Garantizar una educación de calidad inclusiva y equitativa, y promover las oportunidades de aprendizaje permanente para todos.
- 5.- Alcanzar la igualdad entre los géneros y empoderar a todas las mujeres y niñas.
- 6.- Garantizar la disponibilidad y la gestión sostenible del agua y el saneamiento para todos.

.....
2. Naciones Unidas. Día mundial de las Telecomunicaciones y de la Sociedad de la Información 17 de mayo. Recuperado de <https://www.un.org/es/observances/telecommunication-day>

- 7.- Asegurar el acceso a energías asequibles, fiables, sostenibles y modernas para todos.
- 8.- Fomentar el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo, y el trabajo decente para todos.
- 9.- Desarrollar infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación.
- 10.- Reducir las desigualdades entre países y dentro de ellos.
- 11.- Conseguir que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles.
- 12.- Garantizar las pautas de consumo y de producción sostenible.
- 13.- Tomar medidas urgentes para combatir el cambio climático y sus efectos (tomando nota de los acuerdos adoptados en el foro de la Convención Marco de las Naciones Unidas sobre el Cambio Climático).
- 14.- Conservar y utilizar de forma sostenible los océanos, mares y recursos marinos para lograr el desarrollo sostenible.
- 15.- Proteger, restaurar y promover la utilización sostenible de los ecosistemas terrestres, gestionar de manera sostenible los bosques, combatir la desertificación y detener y revertir la degradación de la tierra, y frenar la pérdida de diversidad biológica.
- 16.- Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles.
- 17.- Fortalecer los medios de ejecución y reavivar la alianza mundial para el desarrollo sostenible³.

.....

3. ONU. Objetivos y metas de desarrollo sostenible. Recuperado de <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>

Durante y después de la pandemia, las TIC serán el motor y punto clave para el crecimiento y reestructura de todas las actividades en distintos ámbitos y esto podemos contrastarlo con el crecimiento, hasta el mes de mayo de 2020, que tuvo el uso de internet.

En México hay 80.6 millones de usuarios de Internet, que representan el 70.1% de la población de seis años o más. Esta cifra revela un aumento de 4.3 puntos porcentuales respecto de la registrada en 2018 (65.8%) y de 12.7 puntos porcentuales respecto a 2015 (57.4 %).

Se estima en 20.1 millones, el número de hogares que disponen de Internet (56.4%), ya sea mediante una conexión fija o móvil, lo que significa un incremento de 3.5 puntos porcentuales con respecto a 2018 y de 17.2 puntos porcentuales en comparación con los resultados de 2015 (39.2 %).

De los 80.6 millones de usuarios de Internet de seis años o más, 51.6% son mujeres y 48.4% son hombres.

Entre 2017 y 2019, los usuarios en la zona urbana pasaron de 71.2% a 76.6%, mientras que en la zona rural el incremento fue de 39.2% a 47.7% de usuarios, de 6 años o más.

Los tres principales medios para la conexión de usuarios a Internet en 2019 fueron: celular inteligente (Smartphone) con 95.3%,; computadora portátil con 33.2%, y computadora de escritorio con 28.9%.

Las principales actividades de los usuarios de Internet en 2019 correspondieron a entretenimiento (91.5%), obtención de información (90.7%) y comunicación (90.6%).

Los usuarios de Internet identificaron como principales problemas al conectarse a la red la lentitud en la transferencia de la información (50.1%), interrupciones en el servicio (38.6%) y exceso de información no deseada (25.5%)⁴.

Al respecto, será interesante ver las cifras posteriores a mayo 2020, periodo en el cual se sumaron diversos sectores nacionales a las modalidades a distancia, el caso referente es sobre la educación en línea y, aquí nos encontramos un completo abismo, pues entre las zonas de ciudad y rurales, en estas últimas, la educación a distancia no es para nada una opción viable, pues existen una serie de factores que inhiben el crecimiento y acercamiento a las TIC.

La pandemia no solo nos muestra la cara de una administración pública empujada a lo digital, nos muestra tristemente la carencia de oportunidades y el crecimiento de la desigualdad, pues ante una carencia de electricidad, conectividad a internet, dispositivos, infraestructura, incluso servicios básicos, muchas personas se verán en el punto de abandonar sus estudios, aquí es donde la brecha digital aumentará.

El planteamiento sobre la situación de desigualdad es materia de preocupación nacional, pues ante un crecimiento de desigualdades, cosa que va en contra de los Objetivos de Desarrollo Sostenible (ODS) y es una premisa de la tecnología, la realidad comienza a tomar otro sentido hacia el verdadero acercamiento tecnológico.

El hecho de tener que migrar al plano tecnológico y de servicios labores a la distancia a raíz de la pandemia, deja en claro que se requieren diversos temas de atención en el sector público.

.....
4. Gobierno de México. ¿Cuántos usuarios de internet somos en México? Recuperado de <https://www.gob.mx/sct/articulos/cuantos-usuarios-de-internet-somos-en-mexico>

Muchas de las dependencias y entidades del gobierno mexicano han migrado a un plano de teletrabajo a distancia, apoyados por la tecnología.

Adaptación Digital, caso PRODECON



Los esfuerzos titánicos para adaptarnos a una nueva normalidad completamente limitada, han traído una serie de planteamientos para realizar mucho con poco. Desde la parte tecnológica esto ha sido un esfuerzo mayor, pues se ha trasladado toda atención y prestación de servicios a la ciudadanía, a un punto de encuentro digital, por medio de telefonía y chats con asesores que a la distancia atienden, según sea el caso, para posteriormente canalizar y dar continuidad de la problemática planteada en el área o áreas que resulten competentes; como medida adicional, el uso de la telefonía ip (protocolo de telefonía por internet), con soluciones de videollamadas y los licenciamientos del gigante tecnológico Microsoft, dejan un punto colaborativo entre funcionarios internos de la Procuraduría, maximizando los esfuerzos por familiarizarse con las nuevas tecnologías y no solo delegando la atención al área informática.

Algunos de los proyectos pendientes se verán reflejados a mediano plazo, con la instauración de la firma electrónica para validar todo tipo de documentación y actuaciones de los servidores públicos de la Procuraduría, así como para que se permita el firmado electrónico de promociones y escritos por parte de los contribuyentes, herramienta con lo que se podrá agilizar y transparentar la atención hacia la ciudadanía.

Como respuesta inmediata a la problemática generada por la falta de atención presencial a los contribuyentes, a raíz del Covid-19, la Procuraduría de la Defensa del Contribuyente con el fin de garantizar el derecho de los contribuyentes para recibir justicia en materia fiscal en el orden federal, a través de la prestación de sus servicios de Orientación, Asesoría, Representación, Defensa legal, Quejas, Acuerdos Conclusivos y Consultas, emitió el Acuerdo General número 003/2020.

En el mismo, se ordenó la suspensión temporal de las actividades presenciales tanto en las oficinas centrales, como en sus delegaciones, con el propósito de acatar la normatividad emitida por autoridades federales sanitarias y la Secretaría de la Función Pública, así como con el propósito de resguardar la integridad y salud tanto de los contribuyentes como de los servidores públicos que laboran en la institución, privilegiando lo que comúnmente se conoce como “trabajo a distancia y en casa”, pero en realidad corresponde a teletrabajo.

Cabe hacer mención que la prestación de los servicios antes mencionados no se vio interrumpida por la pandemia, ya que haciendo uso precisamente de las TIC, de inmediato se implementó la prestación integral de los servicios antes referidos por vía remota, ya que si bien aquellos como los de Orientación y Asesoría, ya se venían proporcionando a través de canales remotos como chat en línea, correo electrónico y llamadas telefónicas.

Lo cierto es que en muchas ocasiones para dar continuidad y seguimiento a trámites que derivaban en servicios como el de Quejas, Representación legal o Acuerdos Conclusivos, resultaba necesario que acudiera el contribuyente o su representante legal para la firma de documentos o entrega de información; sin embargo, implementando de lleno a las TIC se privilegió el envío, entrega y recepción de documentación e información, a través de los mencionados canales de comunicación, generando accesibilidad y seguridad a los contribuyentes.

Con la prestación de la totalidad de los servicios vía remota, se advirtió la necesidad de brindar a los contribuyentes una atención más detallada y específica respecto de trámites que, por la complejidad de su problemática, pueden generar algún error o imprecisión en la presentación de las declaraciones de impuestos, de un caso de aclaración, o incluso en la presentación

de un medio de defensa como el recurso de revocación en línea en el portal del Servicio de Administración Tributaria (SAT), lo que implicaría consecuencias negativas para el contribuyente.

Para este tipo de casos se implementó la Asesoría mediante video conferencia, cuando el asesor de **PRODECON** detecta que el contribuyente lo requiere por su condición o complejidad particular de la problemática (principalmente adultos mayores y/o personas sin experiencia en el uso del portal del SAT) con lo que se garantiza la eficacia en la prestación del servicio solicitado, con esta acción se logra dar una atención garante y directa.

Asimismo, con el objetivo de agilizar el proceso de notificación y recepción de información en el trámite del servicio de Queja, cuando en éste se involucra alguna orden de inmovilización de depósitos bancarios de los contribuyentes, mediante el uso de las TIC, el *Ombudsperson* fiscal y la Comisión Nacional Bancaria y de Valores (CNBV), implementaron el intercambio de información mediante un aplicativo en el sistema informático de la Procuraduría, con lo que se mejora el tiempo de atención y se reducen los costos relacionados con dichos trámites, respetando y aplicando así el principio de austeridad en el gasto público.

La Procuraduría de la Defensa del Contribuyente también acordó con algunas autoridades fiscales federales, la recepción y atención de los trámites recibidos y notificados mediante correo electrónico, así como la rendición de los informes respectivos por la misma vía, lo que además de acortar los tiempos de atención, también reduce costos en la operación de los servicios.

Sumado a lo anterior, como parte del programa de Cultura Contributiva, **PRODECON** ha priorizado la impartición

de diversos cursos y talleres tipo webinar dirigidos a los contribuyentes sobre temas fiscales básicos o novedosos, en los que se abordan temas de interés general, como lo fue la campaña “Declara en tu casa”, para coadyuvar a la presentación de la declaración anual para personas físicas, así como otros temas principales de las reformas fiscales que entraron en vigor en este 2020.

De igual forma, mediante diversos webinar dirigidos a los servidores públicos de la Procuraduría, se imparten cursos de actualización y capacitación para poder brindar un servicio profesional y de excelencia a los contribuyentes.

La nueva normalidad dentro de **PRODECON** dará la pauta para un esquema de cambios y reestructuración para adaptarse y, con ello, cada uno de los funcionarios que participan diariamente en las labores, deben mirar con buenos ojos a la tecnología, asimilarla, adaptarse, adentrarse y descubrir de propia mano las múltiples capacidades que con ella puede tener y, no mostrarse reacio ante sus usos.

Las redes sociales se han convertido en el nuevo espacio de convergencia entre dependencias y entidades de gobierno, y ciudadanía, es por ello que el primer canal de consulta se migra al plano digital para solicitar información, identificar trámites, servicios, cuando no es posible visitar presencialmente las oficinas.

Se requiere, por lo tanto, dejar de tomar a la ligera las publicaciones en redes sociales, pues basta con un error humano para que la dependencia o entidad sea marcada por alguna publicación fuera de lugar; sin políticas internas correctamente matizadas e implementadas sobre redes sociales por cada ente de gobierno, no se puede hablar de una correcta atención ciudadana.

La cadena digital comenzará desde el funcionario público como usuario y terminará en el ciudadano como usuario, la presencia digital se vuelve una completa necesidad.

Este último planteamiento no solo aplica para las filas internas de la Procuraduría, también es un contexto ejemplar para adoptar en la administración pública, que pese a las limitaciones deberán mantenerse a flote, con el profesionalismo y la ética que las personas esperan.

Hablemos de algunos puntos carentes, casi utópicos e inexistentes en algunos casos, las perspectivas de uso tecnológico en un entorno post pandemia, los temas a desarrollar en un escenario cercano donde la tutela de los Derechos Humanos se ve reflejada en Derechos Digitales para los usuarios, pues, con un marco de conocimiento podemos dejar en claro como organismo, que se puede hacer mucho de esto y así, a largo plazo, estandarizar un reconocimiento digital de derechos y protección a todo usuario dentro del marco normativo mexicano.

El desarrollo de la política pública que llevó a México a una transformación de implementación tecnológica, tiene como hecho clave el surgimiento de la Estrategia Digital Nacional (EDN)⁵, que salió a la luz en el año 2013.

La Estrategia Digital Nacional es el plan de acción que el Gobierno de la República implementó durante los 5 años siguientes, a partir del 2013, para fomentar la adopción y el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) e insertar a México en la Sociedad de la Información y el Conocimiento.

.....
5. Gobierno de México. 2013-2018. Estrategia Digital Nacional. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf

Dicha estrategia surgió en el marco del Plan Nacional de Desarrollo 2013-2018, ya que formó parte de la estrategia transversal “Gobierno Cercano y Moderno”. En ella se plantearon los desafíos que México enfrenta en el contexto digital y la manera en la que se les haría frente, a través de cinco grandes objetivos:

- 1) Transformación Gubernamental
- 2) Economía Digital
- 3) Transformación del Modelo Educativo
- 4) Salud Universal y Efectiva
- 5) Innovación Cívica y Participación Ciudadana

El propósito fundamental de la Estrategia era lograr un México Digital en el que la adopción y uso de las TIC maximicen su impacto económico, social y político en beneficio de la calidad de vida de las personas. La evidencia empírica ha mostrado que la digitalización –entendida como el concepto que describe las transformaciones sociales, económicas y políticas asociadas con la adopción masiva de las TIC–, impacta el crecimiento del Producto Interno Bruto, la creación de empleos, la productividad, la innovación, la calidad de vida de la población, la igualdad, la transparencia y la eficiencia en la provisión de servicios públicos.

La Estrategia surgió como respuesta a la necesidad de aprovechar las oportunidades que la adopción y el desarrollo de las TIC crean para potenciar el crecimiento del país. De acuerdo con el índice de digitalización establecido en el Programa para un Gobierno Cercano y Moderno, publicado en el Diario Oficial de la Federación el 30 de agosto de 2013, México se encontraba en la última posición en digitalización entre los países de la OCDE, y en la quinta posición en América Latina, con un valor de 37.05 puntos para el año 2011.

A partir de tal escenario, se planteó como meta que México alcanzara en el índice de digitalización, establecido en el Programa para un Gobierno Cercano y Moderno, el promedio de los países de la OCDE para el año 2018. Paralelamente se planteó que México alcanzara los indicadores del país líder de América Latina (actualmente, Chile) para el año 2018.

Para lograr esta meta, y cada uno de los cinco objetivos de la Estrategia Digital Nacional, se plantearon cinco habilitadores claves, que son las siguientes herramientas transversales:

- 1) Conectividad
- 2) Inclusión y Habilidades Digitales
- 3) Interoperabilidad e Identidad Digital
- 4) Marco Jurídico
- 5) Datos Abiertos

El punto pertinente y transversal es sobre la transformación gubernamental que se buscaba con la EDN, cuyas líneas de acción en su momento abrieron el diálogo para dar participación a la ciudadanía en la creación de políticas públicas, el impulso a un gobierno abierto y electrónico. Con ello podemos ver materializados los esfuerzos en una plataforma gubernamental hacia la ciudadanía e intergubernamental para continuar en conjunción de las demás dependencias y entidades gubernamentales.

Hasta hoy, 2020, sigue vigente el Catálogo Nacional de Trámites y Servicios a través de Ventanilla Única Nacional (VUN); regulado en las Disposiciones Generales para la implementación, operación y funcionamiento de la Ventanilla Única Nacional⁶, que en el año 2015, buscaba migrar hacia un plano digital y con

.....

6. Gobierno de México. DOF 04/06/2015. Disposiciones Generales para la implementación, operación y funcionamiento de la Ventanilla Única Nacional. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5395238&fecha=04/06/2015

ello tener un acercamiento ciudadano mayor, pues gracias a la VUN, muchos de los servicios y presencia web están al alcance de la población.

El documento se divide en cinco grandes rubros, los cuales son:

- De la unidad de gobierno digital.
- De las dependencias, entidades y empresas productivas del estado.
- Del catálogo.
- De la información del gobierno.
- De los planes de trabajo para la digitalización de trámites.

Entre los contenidos, se contempla uno de los argumentos anteriormente expuestos sobre el uso de redes sociales y es que, es rescatable la figura del administrador encargado del manejo de cuentas en redes sociales, responsable de los contenidos, también conocido como *“community manager”*, dándole la importancia debida para toda la administración pública.

En julio de 2018, se publicó el Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias⁷.

Entre sus contenidos principales sobre adiciones, nos encontramos con la forma de adquisición para contrataciones, arrendamientos, adjudicaciones con la creación y denominación de una Unidad de Tecnologías de la Información y Comunicación abreviada como UTIC, por la cual debería pasar toda

.....

7. Gobierno de México. DOF 23/07/2018. Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5532585&fecha=23/07/2018

información e interés para la puesta en funcionamiento de algo nuevo (software o hardware) dentro de cualquier dependencia o entidad gubernamental.

Sobre el uso de Firma Electrónica FIEL, su relevancia es incuestionable ya que actualmente en **PRODECON**, se está gestionando su implementación, lo cual facilitará tanto a los servidores públicos de dicha dependencia como a los contribuyentes que acuden a la misma, el poder suscribir electrónicamente los documentos que emitan, lo cual nos suma a diversas entidades federativas, dependencias y organismos públicos descentralizados. A pesar de estas acciones, la transformación digital al porcentaje total no es todavía una realidad.

Hacia finales del año 2019, el tema relacionado con las TIC fue plasmado en el Reglamento de la Oficina de la Presidencia de la República⁸, cuyo artículo 36 hace referencia a la EDN; mismo que se transcribe a continuación:

“Artículo 36. La Coordinación de Estrategia Digital Nacional tiene las atribuciones siguientes:

I. Elaborar y coordinar la Estrategia Digital Nacional, así como desarrollar tecnologías de la información y comunicación para su utilización por parte de la Administración Pública Federal;

II. Dar seguimiento y evaluar periódicamente a las dependencias y entidades competentes de la Administración Pública Federal respecto de la implementación que les corresponda de la Estrategia Digital Nacional;

III. Definir y coordinar las políticas y programas de gobierno digital de la Administración Pública Federal, promoviendo

.....
8. Gobierno de México. DOF 09/12/2019. Reglamento de la Oficina de la Presidencia de la República. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09/12/2019

la innovación, apertura, transparencia, colaboración y participación ciudadana para mejorar la inclusión digital;

IV. *Orientar la emisión y ejecución de políticas públicas y lineamientos, así como los mecanismos de implementación, que deriven de la Estrategia Digital Nacional en materia de tecnologías de la información y comunicación, en coordinación con las dependencias y entidades competentes de la Administración Pública Federal;*

V. *Sugerir a las Unidades de Administración y Finanzas y Oficinas Mayores, según corresponda, de cada dependencia y entidad de la Administración Pública Federal, los nombramientos, ratificaciones y remociones de los titulares o equivalentes de las unidades administrativas encargadas o relacionadas con la informática y las tecnologías de la información y comunicación;*

VI. *Coordinar acciones y, en su caso, suscribir convenios de colaboración con órganos constitucionales autónomos, gobiernos de las entidades federativas y municipios, poderes Legislativo y Judicial de la Federación y de las entidades federativas, instituciones privadas, públicas, nacionales e internacionales y con la sociedad en general, cuya finalidad sea la de impulsar el uso y aprovechamiento de la informática, gobierno digital y tecnologías de la información y comunicación;*

VII. *Emitir recomendaciones, al interior de la Administración Pública Federal, con la participación de las dependencias y entidades competentes, respecto de las mejores prácticas susceptibles de desarrollar e implementar a través de proyectos e iniciativas estratégicas en materia de tecnologías y seguridad de la información;*

VIII. *Participar, en coordinación con las dependencias y entidades de la Administración Pública Federal competentes,*

en el diseño y formulación de las especificaciones y estándares para las adquisiciones y arrendamientos de bienes o servicios de tecnologías de la información y comunicación;

IX. *Colaborar con la Oficialía Mayor de la Secretaría de Hacienda y Crédito Público en las medidas para mejorar la coordinación de las personas titulares de las unidades administrativas estratégicas de informática, tecnología, protocolos de seguridad de la información y comunicación de cada dependencia y entidad de la Administración Pública Federal;*

X. *Requerir a las dependencias y entidades de la Administración Pública Federal la información necesaria para el desarrollo de sus funciones;*

XI. *Colaborar con las unidades administrativas competentes de las dependencias y entidades de la Administración Pública Federal, en la elaboración de las opiniones técnicas para la instrumentación de las políticas sobre el uso y adquisición de programas, bienes informáticos y tecnológicos, y desarrollos informáticos;*

XII. *Presentar opiniones técnicas a la Secretaría de Hacienda y Crédito Público, cuando así lo solicite, para la elaboración de la política nacional de fomento a las compras con proveedores en materia informática y tecnologías de la información y comunicación, destinadas al uso de las dependencias y entidades de la Administración Pública Federal;*

XIII. *Delegar facultades en servidores públicos subalternos, sin perjuicio de su ejercicio directo, mediante acuerdos que deberán ser publicados en el Diario Oficial de la Federación;*

XIV. *Instrumentar los mecanismos de coordinación con las dependencias y entidades de la Administración Pública Federal, para que coadyuven al cumplimiento de las políticas*

en materia de informática, gobierno digital y, en general, de tecnologías de la información y comunicación;

***XV.** Validar los programas de desarrollo informático de la Oficina de la Presidencia;*

***XVI.** Emitir, en su caso, disposiciones administrativas, manuales, guías, instructivos y demás instrumentos análogos para el desarrollo de sus funciones, y*

***XVII.** Las demás que le confieran otros ordenamientos aplicables y aquellas funciones que le encomiende el Presidente”⁹.*

Con la intención de poder modificar e integrar a corto plazo la contemplación de derechos digitales para los usuarios, resulta relevante analizar el caso de España, como un ejemplo y referente en temas afines a lo digital.

En su Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales¹⁰, se contemplan diecisiete Derechos Digitales, que se definen en su apartado pertinente, entre los cuales encontramos temas sobre videovigilancia, derecho a la desconexión, neutralidad en la red, educación digital, ciberseguridad, entre otros.

Establecidos con una garantía en pro del usuario, para dejar en claro la importancia y relevancia al tema, se denomina al Título X, Garantía de los Derechos Digitales:

“...

Artículo 79. *Los derechos en la Era digital. Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España*

9. Ídem

10. Gobierno de España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recuperado de <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>.

sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet. Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.*

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital. Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.*

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales. Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet

y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales. Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio. En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.*

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la

negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese

al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes,

acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet. Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.*

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza

e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos

sobre el mantenimiento de los datos por el servicio. Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.* Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible. Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las

instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones. El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la

solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público;

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad¹¹.

...”

España se convierte en un ejemplo sobre este tema, al incorporar en un instrumento legislativo la tutela de los Derechos Digitales, sin duda vale la pena comenzar a impregnarnos de estas nuevas garantías nacidas a raíz de una sociedad informatizada, ya que somos entes digitales, humanos trasladados al plano intangible cuyos defectos y virtudes se contextualizan por medio de dispositivos, texto, iconos y contenido multimedia, dejando ver un reflejo del mundo material a través de las TIC.

Para el caso de México, no encontramos ningún tipo de legislación que identifique como tal a los Derechos Digitales garantizando su ejercicio, quizá solo encontramos algunas derivaciones y particiones seccionadas como pequeños apartados en distintas leyes.

.....
11. Íbidem.

Contrastando Derechos Digitales



Comencemos a ampliar el panorama, al mencionar que Internet tiene características de servicio público. Personas, comunidades, autoridades públicas y entidades privadas dependen cada vez más de Internet para sus actividades y tienen una expectativa legítima de que sus servicios sean accesibles, ofrecidos sin discriminación, asequibles, seguros, fiables y continuos. Además, nadie debería estar sujeto a injerencias ilícitas, innecesarias o desproporcionadas en el ejercicio de sus Derechos Humanos y sus libertades fundamentales al usar Internet. Los usuarios deberían recibir apoyo para comprender y ejercer de manera efectiva sus Derechos Humanos en Internet en el caso de que sus derechos y libertades hayan sido objeto de restricción o injerencia. Tal apoyo debería incluir orientación sobre el acceso a recursos efectivos. A la luz de las oportunidades que brinda Internet en términos de transparencia y responsabilidad en la gestión de los asuntos públicos, los usuarios deberían poder usar Internet para participar en la vida democrática¹².

Identifiquemos algunas definiciones más intrínsecamente relacionadas con los Derechos Digitales.

Acorde al World Economic Forum (WEF), los Derechos Digitales son básicamente derechos humanos en la era de Internet. Los derechos a la privacidad en línea y la libertad de expresión, por ejemplo, son en realidad extensiones de los derechos iguales e inalienables establecidos en la Declaración Universal de Derechos Humanos de las Naciones Unidas. Según la ONU, desconectar a las personas de Internet viola estos derechos y va en contra del derecho internacional¹³.



12. Consejo de Europa. 2014. Recomendación CM/Rec(2014)6 y exposición de motivos. GUÍA DE LOS DERECHOS HUMANOS PARA LOS USUARIOS DE INTERNET. Recuperado de <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cc3b7>

13. World Economic Forum. 2015. What are your digital rights?. Recuperado de <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/>

Otra definición amplia y acertada nos indica que: Los derechos son una parte inalienable de la sociedad que determinan la dinámica de la convivencia.

Están, por ejemplo, los derechos inherentes que son los que tiene cualquier individuo por el sólo hecho de serlo.

Sin embargo, hay que recordar que los derechos no siempre han sido los mismos. La historia y el cambio constante en las sociedades moldea muchos de ellos.

El término **Derechos Digitales** alude a los permisos de las personas para realizar acciones legítimas que comprenden el uso de:

- Un ordenador.
- Todo tipo de dispositivo electrónico, o
- una red de comunicaciones.

El término tiene estrecha relación con la protección y cumplimiento de otros derechos existentes, tales como el derecho a la privacidad o la libertad de expresión, en el ámbito de las nuevas tecnologías digitales, especialmente Internet.

Estos derechos tienen como finalidad la protección de las personas que utilizan las diferentes herramientas digitales, con el fin de evitar las discriminaciones. Se refiere principalmente a los individuos que, ya sea por problemas económicos o por la localización geográfica, tienen limitado el uso de esas herramientas¹⁴.

.....
14. Ayuda Ley Protección de Datos. 2018. Derechos Digitales. Recuperado de <https://ayudaleyprotecciondatos.es/2018/10/03/derechos-digitales/>

Con el concepto anterior queda más claro que estos nuevos derechos, los que muchos llaman derechos de cuarta generación, nacen en la cuna de las tecnologías, donde la sociedad depende de las TIC y el internet se vuelve un canal fundamental.

Muchas ciudades en el mundo se suman al decir que, Internet se ha convertido en inseparable de nuestra vida cotidiana. Sin embargo, todos los días, se presentan nuevos casos de abuso de los Derechos Digitales, uso indebido y desinformación y concentración de poder en todo el mundo: se censura la libertad de expresión; la información personal, incluidos nuestros movimientos y comunicaciones, es monitoreada, compartida y vendida sin consentimiento; algoritmos de ‘caja negra’ que se utilizan para tomar decisiones irresponsables; las redes sociales se utilizan como herramienta de acoso y discurso de odio; y los procesos democráticos y la opinión pública están siendo socavados.

Los gobiernos, como entes democráticos más cercanos a las personas, debieran estar comprometidos a eliminar los impedimentos para aprovechar las oportunidades tecnológicas que mejoran las vidas de su población y a brindar servicios e infraestructuras digitales confiables y seguros que apoyen a nuestras comunidades. Creemos firmemente que los principios de Derechos Humanos como la privacidad, la libertad de expresión y la democracia deben incorporarse por diseño en las plataformas digitales, comenzando por las infraestructuras y los servicios digitales controlados localmente¹⁵.

Podemos construir con todos los elementos una definición propia de Derechos Digitales, al decir que son una serie de

.....
15. Cities for Digital Rights. Declaration of Cities Coalition for Digital Rights. Recuperado de https://citiesfordigitalrights.org/assets/Declaration_Cities_for_Digital_Rights.pdf

garantías de protección para el usuario, el reconocimiento de una identidad digital cuya importancia se ve reflejada en el mundo material, con lo cual adquiere derechos inherentes a los Derechos Humanos, pero reflejados en el plano intangible del ciberespacio.

Retomemos un poco de los artículos referidos anteriormente y hagamos una comparación generalizada sobre lo que contamos en México, para el caso de la administración pública, la cual deberá prestar la debida importancia, pues es una realidad en el mundo que hoy en día usamos a la tecnología, o no existimos.

Neutralidad en la red

Uno de los temas más controversiales en el mundo y particularmente en el continente americano ha sido el de neutralidad en la red, este concepto es referente al derecho que nos permite como usuarios poder navegar libremente por internet: sin censura, visualizando contenidos limitados o imperados; caso contrario a lo que se vive digitalmente en países como Venezuela o China, en donde la neutralidad en la red no existe y el régimen digital se impera al usuario, lo cual sesga la libertad de expresión y navegación.

Estados Unidos, tuvo un caso muy controversial en donde la Federal Communications Commission (FCC), órgano regulador de comunicaciones en el país vecino del norte, recibió presión presidencial para acabar con la neutralidad en la red, lo cual desató múltiples levantamientos por parte de usuarios y autoridades; hasta la fecha algunos estados siguen en pie de lucha, mientras que otros más han recuperado su neutralidad en la red.

La neutralidad en la red como derecho digital, cobra una total relevancia para el usuario en diversos sentidos, podemos contrastarla con la televisión por pago, pues para gozar de algunos contenidos el usuario que contrata el servicio debe ampliar su paquete para disfrutarlos; con la neutralidad en la red podemos acceder en este momento a todo en internet, sin necesidad de tener que costear por el acceso a un buscador, a un sitio multimedia, etc.

No se deben confundir los servicios adicionales de pago de compañías particulares o los servicios premium, con la afectación a la neutralidad en la red. Son cosas distintas.

Para el caso de nuestro país, en este año el órgano regulador de telecomunicaciones, Instituto Federal de Telecomunicaciones (IFT), realizó diversas consultas abiertas a usuarios con relación a la neutralidad en la red, pues ese derecho que tenemos lo ejercemos día a día.

México requiere un precepto legal explícito en donde se garantice el derecho digital a la neutralidad en la red.

Por parte de cada una de las entidades gubernamentales, la neutralidad en la red muchas veces se ve ciertamente opacada al ceder a las configuraciones imperadas por el fabricante de soluciones en seguridad, el ejemplo no va tan lejos; el uso del navegador The Onion Router (TOR), una herramienta especializada en cifrar la navegación y utilizar redirecciones a otros países, para muchos presupone un riesgo a la ciberseguridad; lo cierto es que todo depende de la óptica, enfoque y conocimiento del usuario final, pues en algunos países censurados ha servido como ente libertador y canal de conexión, no es más que un mal estereotipo que este navegador solo sea utilizado para fines delictivos.

La censura en sitios supuestamente peligrosos a través de un cortafuegos de red gubernamental. discrepa mucho entre cada uno de los proveedores de este servicio, se requiere una homologación para crear una verdadera lista de navegación para los funcionarios públicos, no solo dejar las configuraciones por defecto.

Eliminar la neutralidad en la red limitaría la libertad de los ciudadanos, los proveedores de servicios de internet podrían irrumpir en la privacidad del usuario para visualizar toda su actividad sin necesidad de una orden judicial, restringir incluso las velocidades y lo dicho sobre el acceso y consumo de contenidos.

Para cerrar el argumento de la importancia de reconocer como derecho humano a la neutralidad en la red, se hace hincapié, particularmente para los casos internos de gobierno, el poder de verdad concientizar al usuario en primera instancia para no tener que limitar con un firewall a la navegación y así poder acceder a todo el contenido que se requiera, sin que se afecte en forma alguna el derecho a la privacidad.

Acceso al internet



Ahora bien, pasemos a un punto que se puede hacer mención para el caso de México, al conocer de algunas de las reformas a la Constitución para garantizar el acceso a Internet en todo el territorio. Si hacemos memoria existió un programa llamado “México Conectado” en donde se planteaba acercar el espectro de Internet inalámbrico a diversos puntos del país, por medio de puntos de enlace de conexión, también llamados hotspot, ubicados en puntos centrales de las ciudades.

Las entidades de gobierno deben comenzar desde sus filas internas a conocer y familiarizarse con las nuevas tecnologías, y desde esta óptica plantear una conjunción como gobierno al acercar una conexión a internet a las personas que requieren sus servicios, sin importar el área geográfica en la que se encuentren.

En la actualidad, ante la rápida propagación del COVID-19 en el mundo, una de las soluciones más efectivas es el aislamiento social a fin de disminuir la transmisión del virus. Esto implica permanecer en casa y evitar la circulación pública en lugares de trabajo, estudio, recreación, entre otros.

En este contexto, aplicaciones digitales que habilitan el teletrabajo, la educación a distancia, la realización de trámites, la interacción social y el esparcimiento, aparecen como una solución para lidiar con estas circunstancias. El factor habilitante para su uso es la conectividad. Sin embargo, en los países de América Latina y el Caribe, la brecha digital deja de manifiesto un nuevo elemento de inequidad, la desigualdad digital¹⁶.

.....
16. CEPAL. 2020. Las oportunidades de la digitalización en américa latina frente al covid-19. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19_es.pdf

Una de las respuestas más efectivas a los momentos que se viven hoy en día, sería que los gobiernos y las empresas ayudaran a cerrar esa brecha digital que tanto hemos mencionado, conectando a los que no están conectados y maximizando las oportunidades para que todos los ciudadanos puedan gozar de los derechos digitales de acceso a Internet.

Ciberseguridad

Abordemos un tema que al menos en este año ha dado mucho de qué hablar, al haber existido diversos incidentes digitales, tanto en la iniciativa privada como en la pública.

De los ataques cibernéticos que se han conocido, figura el ataque de ransomware, un tipo de malware que se encarga de cifrar todos los archivos de un dispositivo, computadora, para posteriormente pedir algún tipo de rescate para la recuperación de la información contenida.

Otro tipo de ataque muy común es el llamado defacement, o desfiguro, el cual consiste en ingresar y pasar el panel de control de administrador para posteriormente desfigurar el sitio web, lo cual crea un desprestigio; usualmente es usado para dejar mensajes y mostrar las capacidades de los ciber atacantes.

También se han visto otros ataques, como el llamado DDoS, una irrupción de denegación de servicio, que consiste en dejar fuera de línea al sitio web, coloquialmente se le conoce como “tirar la página”.

Por si fuera poco, en algunos casos se generaron ataques cibernéticos en donde, mediante un buscador especializado (shodan), se podía visualizar y obtener diversa información personal o clasificada como reservada.

Desde la trinchera personal de **PRODECON**, todos los ataques cibernéticos recibidos para intentar lograr alguna acción mayor, se han logrado mitigar, a veces los intentos son diarios y continuos, persistentes, pero sin lograr su cometido.

Y por lo anterior es que la seguridad en materia digital o, en este caso ciberseguridad, al cubrir una diversidad de ramas y aspectos, se hace un punto completamente necesario como Derecho Digital, no solo para los usuarios si no para los actores de gobierno.

La ciberseguridad es una rama transversal, multidisciplinaria, en donde comienza todo con el usuario y termina todo con el usuario, en un ciclo en donde la prevención se convierte en el eslabón más fuerte que se le puede ofrecer al sistema.

Al menos en la parte de la administración pública, el tema de la seguridad sigue siendo delegado a los cuerpos informáticos, mientras que el usuario no tiene ni la más mínima importancia hacia lo que podría ser un verdadero factor de prevención; por ello, se requieren campañas de difusión que promuevan una sensibilización tecnológica a la par de buscar un entorno de teletrabajo seguro, pues, un atacante puede ingresar más fácilmente a la red de la víctima desde casa e interceptar datos como contraseñas gubernamentales, tomar el control del dispositivo móvil o computadora, entre otros.

Trabajar desde una red casera con información confidencial es un riesgo, es por ello que, a manera de ejemplo, en la Procuraduría de la Defensa del Contribuyente, como primera acción se plantearon medidas para los entornos de trabajo a distancia, contemplando la situación sobre la atención a los contribuyentes por vía remota y el poder seguir con las labores que ello implica, pero vía remota.

Algunas de las medidas planteadas se dividieron en rubros, generalizando los puntos importantes para mantener un usuario y equipo seguro, lo cual dependerá de la aplicación e importancia que le den.

Sobre el manejo de equipos de cómputo:

- Los equipos deben ser desconectados con apoyo de soporte local, garantizando que el equipo y periféricos se encuentren en buen funcionamiento y sin daños.
- Sobre el traslado, el usuario debe comprometerse a tener los mayores cuidados, evitando golpes, rayaduras y/o afectaciones.
- El lugar final a donde será instalado el respectivo equipo debe contar con las mínimas condiciones ambientales, garantizando la integridad y el buen funcionamiento de éste.
- El usuario se compromete a su colocación, conexión y cuidados generales.

Sobre el manejo de dispositivos periféricos:

- Entendamos como dispositivos periféricos todos los aditamentos externos al equipo, memorias, cámaras, micrófonos, en general, dispositivos de conexión USB u otras.

El usuario deberá evitar conectar dispositivos periféricos ajenos a la situación laboral directa con **PRODECON**, aquellos que no tengan alguna función directa en sus actividades y aquellos que representen un riesgo o distracción al equipo.

- Sobre las memorias USB, se hace hincapié en utilizar únicamente dispositivos laborales conocidos, evitando ingresar periféricos USB de almacenamiento que puedan contener potenciales amenazas, como *malware*.
- En caso de no contar con una tarjeta de red interna para el dispositivo laboral, el usuario debería adquirir una y realizar las configuraciones pertinentes.

Sobre el manejo de redes:

- Se configurará el equipo para compartir una conexión de acceso tipo Red virtual privada (VPN) directa a la Procuraduría, por lo cual se aconseja utilizarla en los horarios previamente establecidos, con la finalidad de evitar saturar a la misma, aun y cuando se puede tener acceso en todo momento.
- Al no tener el equipo un *firewall* de protección, la responsabilidad de navegación es completa del usuario, por lo que se sugiere evitar a toda costa, sitios de descarga de *malware*, sitios para adultos, sitios de juegos, sitios de apuestas, sitios con contenido de seguridad delicado, entre otros.
- Se recomienda configurar su red casera con los máximos controles de seguridad, cambiando la contraseña por default, así como el nombre de la red, y desactivando los accesos Wi-Fi Protected Setup (WPS), los cuales vienen por default en las configuraciones y permiten agilizar la conectividad de dispositivos, lo cual se convierte en un riesgo, pues existen aplicaciones que pueden lograr una conexión en cuestión de segundos y sin permiso del dueño de la red.

Sobre el manejo de información:

- Al estar en un entorno de trabajo a distancia, las medidas sobre la información manejada deben tener consideraciones de resguardo para no ser filtrada o, en su caso, dañada.
- El usuario se compromete a hacer buen uso de la información, y respaldarla constantemente.
- El usuario se compromete a no divulgar la información laboral, así como a resguardar sus contraseñas.

Sobre el manejo de ciberincidentes:

- Para evitar ser víctima de un daño digital, se recomienda utilizar un software encargado de eliminar todas amenazas digitales que podrían infectar un dispositivo, también conocido como antimalware.
- La limpieza del equipo debe ser semanal, eliminando cookies, cache y amenazas potenciales que sean detectadas.

Sobre el trabajo a distancia o teletrabajo:

El COVID-19 nos deja un aprendizaje sobre la importancia del teletrabajo y la necesidad de la ciberseguridad, lo que debe ser un Derecho Digital.

En la traducción de un estudio reciente sobre nuestro país, México: Cyber Threat Landscape, encontramos que: (fuente)

México es una de las principales economías emergentes de la región y, como tal, atrae la atención de actores hostiles para explotar a las organizaciones vulnerables en el país.

Los bancos y las instituciones financieras han sido los principales objetivos de actores hostiles.

- El delito cibernético es la principal amenaza, que debería continuar en el futuro previsible.
- Se han conocido casos de ciber espionaje dirigido a intereses mexicanos. Tal actividad depende en gran medida de la intención de los actores que buscan determinar la posición del gobierno sobre cuestiones geopolíticas, y fluirá y refluirá en consecuencia.

- El hacktivismo es un medio viable de protesta social que históricamente se ha dirigido a algunas entidades gubernamentales y, probablemente, continuará en el futuro.

Desafortunadamente, las dependencias y entidades gubernamentales mantienen información limitada para brindar más fidelidad a las estadísticas de actividad cibernética hostil. Dicho esto, en el contexto mexicano actual, no existe ley que exija a las organizaciones, públicas o privadas, informar sobre las infracciones o ataques cibernéticos que hubieran sufrido, por lo que esas estadísticas, incluso si estuvieran disponibles, no serían del todo confiables¹⁷.

América Latina tiene una penetración de Internet muy alta, pero parece que en gran medida no está totalmente preparada para contrarrestar a las amenazas de ciberseguridad.

.....
17. Lookingglass Cyber Solutions. 2018. Mexico: Cyber Threat Landscape. Recuperado de https://www.lookingglasscyber.com/wp-content/uploads/2019/03/STRATISS-Cyber_Landscape_Mexico.pdf

Protección a menores en las TIC



Sobre la protección a menores en Internet, como lo refiere el Derecho Digital español, al hacer el contraste hacia México, podemos advertir que no contamos, como tal, con un instrumento legal para que los padres o tutores tengan medidas de ciberprotección hacia los menores en el tema de dispositivos e, incluso, muchas veces son desconocidos los parámetros y recomendaciones de cuidados y buenos hábitos en Internet.

Por ello, Europol emitió lo siguiente:

El impacto global de COVID-19 significa que las personas pasan más tiempo en línea. Esto incluye tanto a niños como a adultos.

Los adultos que trabajan de forma remota son menos capaces de pasar tiempo con sus hijos, a quienes se les permite un mayor acceso a Internet sin supervisión. Como resultado, los niños son:

- Más expuestos a los delincuentes a través de juegos en línea, el uso de grupos de chat en aplicaciones, intentos de phishing por correo electrónico, contacto no solicitado en redes sociales y a través de aplicaciones educativas en línea menos seguras;
- Más inclinado a hacer material explícito para intercambiar con sus compañeros, llegando eventualmente a los delincuentes sexuales infantiles;
- En algunos casos, sentirse solo y aislado, de lo que los agresores intentan beneficiarse, conectándose con ellos para producir material explícito o para concertar un encuentro en la vida real¹⁸.



18. EUROPOL. 2020. COVID-19: Child sexual exploitation. Recuperado de <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation>

Migrar hacia un plano digital no solo es cuestión laboral, los infantes utilizan a las TIC como medio de ocio, y están presentes en todo sentido de su vida.

Uno de cada tres usuarios de internet en todo el mundo es un niño. Es probable que esta proporción sea aún mayor en el Sur global. Las organizaciones que trabajan para promover los derechos del niño y promover el bienestar deben comprender cómo reducir el riesgo de daño que enfrentan los niños en línea, mientras maximizan sus oportunidades de aprendizaje, participación y creatividad.

Fundamentalmente, las perspectivas y experiencias de los niños deben tenerse en cuenta al redactar las políticas que rijan el uso de tecnología digital a los jóvenes, así como al diseñar la tecnología en sí. Sin embargo, todavía hay pruebas insuficientes a nivel mundial para permitir que las políticas y la práctica actúen en el mejor interés de los niños.

Para cerrar esta brecha de evidencia, la Oficina de Investigación de UNICEF - Innocenti coordina y facilita la investigación sobre el uso de tecnologías digitales por parte de los niños mediante el desarrollo de metodologías de investigación que se pueden implementar para generar evidencia nacional. UNICEF Innocenti coordina dos programas de generación de evidencia en varios países, *“Global Kids Online”* y *“Disrupting Harm”*, que sirven para generar evidencia de las oportunidades y riesgos que los niños de todo el mundo pueden encontrar en la era digital.

Además, la Oficina de Investigación de UNICEF - Innocenti colabora con las partes interesadas para garantizar que las perspectivas de los niños estén en el centro del discurso y los debates sobre la gobernanza de Internet y el uso de Internet por parte de los niños¹⁹.

.....
19. UNICEF. 2020. Child rights in the digital age. Recuperado de <https://www.unicef-irc.org/research/child-rights-in-the-digital-age/>

La conjunción para sumar esfuerzos entre entidades gubernamentales, a la par de sumar sociedad civil y sector particular, en pro de la prevención ante daños digitales a menores, es otro de los puntos a considerar; es necesario un punto de contemplación legislativo para que éste nuevo derecho digital tenga garantías y atención.

Sobre los datos personales



Para fortuna en México, tenemos al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como órgano garante en materia de protección de datos personales. Dentro de los Derechos Digitales, como particulares, el tener un punto de protección para toda la información generada por cada usuario es una necesidad y de vital importancia para no ser víctima de un delito mayor.

El INAI es el organismo constitucional autónomo encargado de facilitar y garantizar el acceso de las personas a la información pública y el acceso y protección de los datos personales, así como de promover la cultura de la transparencia en la gestión pública y la rendición de cuentas del gobierno a la sociedad²⁰.

La identidad digital de una persona cuando llega al ciberespacio, requiere algunos planteamientos para atender, como qué datos genera, en qué portales, cuáles serán los usos, las medidas de protección, principalmente²¹.

El derecho a la protección de los datos personales se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, como un Derecho Humano Fundamental.

El derecho a la protección de datos personales incluye a su vez el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (Derechos ARCO),

.....

20. Gobierno de México. 2020. INAI. Recuperado de <https://www.gob.mx/sfp/documentos/instituto-nacional-de-transparencia-acceso-a-la-informacion-y-proteccion-de-datos-personales-inai>

21. Gobierno de México. DOF 29/01/2016. Decreto por el que se declaran reformadas y derogadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de la reforma política de la Ciudad de México.

que para su efectivo ejercicio es necesario solicitarlo ante el responsable que trata los datos personales²².

Es de suma importancia conocer este punto, pues contamos con un Derecho Digital reconocido en el marco constitucional y, así como éste, esperemos pronto ver algunos otros derechos digitales más con un respaldo legal y, quizá, alguna entidad de gobierno que pueda encargarse de que se haga valer su debido ejercicio.

Las dependencias y entidades gubernamentales tienen que apegarse a lo indicado en la Ley, para el resguardo, manejo, uso final e implicaciones en materia de datos personales; aquí es donde nos encontramos con un concepto relacionado: la transparencia.

El Gobierno de México ha habilitado plataformas digitales para garantizar que los procesos de adquisición, contratación y todo lo relacionado con dichos temas, sean verificables por la ciudadanía interesada, dando a conocer montos, proveedores, necesidades y todo lo involucrado con ello.

Otro punto a conocer de la transparencia en México, es el acceso que puede tener un ciudadano mediante solicitudes información. Aquí hablaremos de la delgada línea entre la realidad y el hecho de solo pedir información, sin más.

Toda información usualmente interna hasta hace algunos años, ahora puede ser comprobada por medios digitales, lo cual deja en un punto abierto y quizá expuesto a las dependencias y entidades de gobierno, pues al muchas veces desconocer temas sobre incidentes de ciberseguridad y lo relacionado

.....
22. Gobierno de México. 2018. Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/428335/DDP_Gu_a_derechos_ARCO_13Dic18.pdf

a tecnologías, podrían ceder información valiosa para posteriormente ser víctimas de un ataque.

¿Hasta qué punto se garantiza transparencia si detrás se busca afectar a un órgano gubernamental?

El concepto en sí es abstracto y cada persona lo definirá y utilizará acorde a sus necesidades imperantes, por ello caer en un punto de homologación para materia de acceso y transparencia que no se vea viciado, debe ser materia de derechos digitales.

La transparencia se ha hecho presente en la lucha contra la corrupción. El Banco Interamericano de Desarrollo hizo un pronunciamiento tajante y abierto para interpretación de cada persona:

“No existe una bala de plata para minimizar los riesgos de fraude y corrupción en situaciones de emergencia. Las soluciones dependen del entramado institucional de cada país y deben nutrirse de varios ingredientes como por ejemplo los requisitos de información sobre beneficiarios finales de las empresas y subcontratistas; el fortalecimiento de las prácticas de auditoría y fiscalización; y la creación de comités especializados para monitorear la utilización de los recursos asociados a las emergencias, entre otros aspectos.

En este contexto, la transparencia y la rendición de cuentas tienen un rol central, especialmente cuando los ciudadanos pueden acceder a información de calidad y actualizada sobre el ciclo de vida de los recursos. Para ello, las herramientas digitales son una buena respuesta al desafío de responder a la crisis con integridad. Estas herramientas permiten integrar

y visualizar datos, identificar posibles anomalías e incrementar la trazabilidad de los flujos de recursos. También permiten monitorear en tiempo real los registros contables, presupuestales, de tesorería y de beneficiarios desde origen del recurso al cierre financiero y administrativo. Además, es posible que cualquier persona comparta información sobre el uso de recursos, lo cual genera la disuasión de actividades ilícitas y facilita la rendición de cuentas”²³.

Todo lo relacionado con protección de datos personales como Derecho Digital, siempre tendrá muchas ópticas y opiniones encontradas, quizá la mayor premisa que debe prevalecer, es siempre buscar la tutela del usuario ya sea un ente de gobierno o un particular, y no caer en un marco donde se busque el consumo y al usuario como producto.

Las legislaciones europeas tutelan al usuario, la legislación de Estados Unidos solo mira al usuario como un producto; recordemos que los datos personales son algo con lo que se puede lucrar, cada información, cada dato, archivo, contenido generado, tiene valor para alguien.

Sensibilizar a toda la población en general sobre el valor de su información es un primer gran punto de partida, internamente en la intuición, establecer lineamientos que se hagan comunes y aplicables, es un primer gran paso.

.....

23. BID. 2020. COVID-19: Transparencia para asegurar políticas efectivas en momentos de crisis. Recuperado de <https://blogs.iadb.org/administracion-publica/es/covid-19-transparencia-como-un-medio-para-asegurar-la-efectividad-de-las-politicas-en-momentos-de-crisis/>

Intimidad y desconexión laboral



La intimidad del trabajador debe ser un Derecho Laboral garantizado desde la cuna de cada centro de trabajo y, para ello, es importante establecer mecanismos que permitan proteger la privacidad y confidencialidad de los datos personales de los trabajadores.

De igual manera, los sistemas de videovigilancia que se utilizan en los centros de trabajo, mismos que deben ser herramientas para el control y monitoreo en áreas comunes, no deben transgredir a los trabajadores. En diversos sitios se han encontrado, hasta la fecha, cámaras instaladas a unos cuantos pasos de cada trabajador, registrando toda acción, en casos más graves, apuntando hacia su computadora para registrar también en video todo lo que realiza.

La vigilancia laboral no solamente aplica para el ámbito de grabar y crear contenidos multimedia, gracias a las funciones de varias herramientas tecnológicas, la geolocalización es simple de realizar y con ello, sin autorización, estamos hablando de una intromisión a la privacidad.

El derecho a la desconexión es otro de los Derechos Digitales que internamente, en cada centro laboral, se debe considerar, respetando y entendiendo que el trabajador es un usuario, un ser humano y no debe ser molestado fuera de las horas laborales; algo que con el trabajo a distancia muchas veces se pierde, puesto que se puede pensar que por el hecho de estar en casa, se está a disposición a toda hora del día, incluso en las madrugadas, lo cual resulta algo ilógico.

Políticas de impulso a los Derechos Digitales

La Estrategia Nacional de Ciberseguridad (ENCS) salió a la luz en el año 2017, se trabajó un año anterior en foros y consultas donde academia, gobierno, empresas y ciudadanía tenían convergencia para la estructuración de esta primera política pública en materia digital que tutelaba a la ciberseguridad.

La Estrategia Nacional de Ciberseguridad es el documento que establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

A. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.

B. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.

C. La necesidad de una cultura general de ciberseguridad.

El aumento de riesgos, amenazas y ataques informáticos sofisticados, el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades, así como el incremento de conductas delictivas que se cometen a través de las TIC, son circunstancias que hacen de la ciberseguridad un tema complejo. A lo anterior, se suma la naturaleza global del ciberespacio y la concurrencia de diferentes soberanías y marcos jurídicos.

El objetivo general de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

Para cumplir con el objetivo general, se establecieron 5 objetivos estratégicos:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

Para el desarrollo de la ENCS se consideraron tres principios rectores:

- A. Perspectiva de derechos humanos.
- B. Enfoque basado en gestión de riesgos.
- C. Colaboración multidisciplinaria y de múltiples actores.

Para alcanzar los objetivos estratégicos se contempló desarrollar 8 ejes transversales:

1. Cultura de ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.

6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento²⁴.

Es cierto que los temas digitales sobrepasan al derecho, sin embargo, las constantes actualizaciones y contemplaciones hacia la tecnología y, ele intentar regular y adaptar el derecho a los avances tecnológicos, son serán la base para la construcción de una sociedad funcional y digitalizada.

.....

24. Gobierno de México. 2017. Estrategia Nacional de Ciberseguridad. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Futuros usos tecnológicos

La cadena de bloques o blockchain, es una serie de registros de datos inmutables con marca de tiempo que es administrada por un grupo de dispositivos que no son propiedad ni recaen en el control de una sola entidad. Cada uno de estos bloques se encuentra protegido y vinculado entre sí mediante principios criptográficos o de cifrado avanzado.

Blockchain no tiene una autoridad central; es la definición misma de un sistema democratizado. Dado que es un libro mayor compartido e inmutable, la información que contiene está abierta para que todos la vean. Por lo tanto, cualquier cosa que se construya en la cadena de bloques es transparente por su propia naturaleza y todos los involucrados son responsables de sus acciones.

Comprender el funcionamiento de blockchain es un tanto complicado para el usuario promedio, sin embargo, las características de inmutabilidad, respaldos directos, claves de cifrado, autorización comprobada, transparencia, son factores que hacen que blockchain sea una tecnología rentable con muchos fines.

Sin duda, blockchain es el mejor respaldo para los procesos democráticos en el mundo, pues hasta la fecha parece inalterable, quizá el mayor enemigo que podría tener, es el uso del cómputo cuántico, pero sería utópico pensar que un usuario promedio tenga acceso a tales capacidades.

Para el caso específico de **PRODECON**, el uso de la tecnología de blockchain sería benéfico para llevar todo un registro inalterable de trámites realizados, acuerdos emitidos, quejas

atendidas y demás atenciones al contribuyente; a la par de que internamente el registro y disponibilidad de toda documentación estaría abierta a consulta para las autoridades pertinentes. La inclusión de blockchain es un refuerzo mayor al que se puede obtener con firmas electrónicas, pensemos en las múltiples posibilidades de aplicación en cuanto a los registros de atención a cada contribuyente.

Otro de los conceptos que ha traído mejoras cuando es implementado, incluso en las casas productoras más grandes como Netflix; es Big Data, consistente en el análisis de grandes volúmenes de datos para obtener y utilizar información en específico. Analicemos algunos de los casos de uso identificados por una casa de soluciones digitales global:

- Desarrollo de productos: empresas como Netflix y Procter & Gamble usan big data para prever la demanda de los clientes. Construyen modelos predictivos para nuevos productos y servicios, clasifican atributos clave de productos anteriores y actuales, y modelan la relación entre dichos atributos y el éxito comercial de las ofertas. Además, P&G utiliza los datos y los análisis de grupos de interés, redes sociales, mercados de prueba y avances de salida en tiendas para planificar, producir y lanzar nuevos productos.
- Mantenimiento predictivo: los factores capaces de predecir fallas mecánicas pueden estar profundamente ocultos entre datos estructurados (año del equipo, marca o modelo de una máquina) o entre datos no estructurados que cubren millones de entradas de registros, datos de sensores, mensajes de error y temperaturas de motor. Al analizar estos indicadores de problemas potenciales antes de que estos se produzcan, las organizaciones pueden implementar el mantenimiento de una forma más rentable y optimizar el tiempo de servicio de componentes y equipos.

- **Experiencia del cliente:** actualmente disponer de una visión clara de la experiencia del cliente es más posible que nunca. El big data le permite recopilar datos de redes sociales, visitas a páginas web, registros de llamadas y otras fuentes para mejorar la experiencia de interacción, así como maximizar el valor ofrecido. Es posible preparar ofertas personalizadas, reducir las tasas de abandono de los clientes y administrar las incidencias de manera proactiva.
- **Fraude y cumplimiento:** en lo que a seguridad se refiere, no se enfrenta a simples hackers solitarios, sino a equipos completos de expertos. Los contextos de seguridad y requisitos de conformidad están en constante evolución. El big data ayuda a identificar patrones en los datos que pueden ser indicativos de fraude, al tiempo que concentra grandes volúmenes de información para agilizar la generación de informes normativos.
- **Aprendizaje autónomo:** el aprendizaje autónomo es un tema candente en la actualidad. Los datos, concretamente big data, es uno de los motivos de que así sea. Ahora, en lugar de programarse, las máquinas pueden aprender. Esto es posible gracias a la disponibilidad de big data para crear modelos de aprendizaje autónomo.
- **Eficiencia operativa:** puede que la eficiencia operativa no sea la noticia más importante, pero es el área en que big data tiene un mayor impacto. Big data permite analizar y evaluar la producción, la opinión de los clientes, las devoluciones y otros factores para reducir las situaciones de falta de stock y prever la demanda futura. Big data también puede utilizarse para mejorar la toma de decisiones en función de la demanda de mercado del momento.
- **Impulsar la innovación:** big data puede ayudar a innovar mediante el estudio de las interdependencias entre seres humanos, instituciones, entidades y procesos, y,

posteriormente, mediante la determinación de nuevas maneras de usar dicha información. Al utilizar las perspectivas que ofrecen los datos para mejorar las decisiones financieras y consideraciones de planificación. Se deben estudiar las tendencias y lo que desean los clientes para ofrecer nuevos productos y servicios, e implementar políticas de precios dinámicas. Las posibilidades son infinitas²⁵.

Las ventajas para la administración pública al usar big data permitirían identificar y atender problemáticas sociales con menor tiempo y esfuerzo, dejando una base de antecedentes de atención en cada una de las dependencias u organismos públicos descentralizados.

Podemos utilizar al SAT de ejemplo, para el caso específico de valerse de algoritmos de big data que se encargan de analizar enormes volúmenes de información para detectar comprobantes fiscales que amparen operaciones inexistentes. En el caso de **PRODECON**, el análisis de volúmenes de datos automatizado podría ayudar a eficientar servicios particularmente hacia el contribuyente, dando un parámetro de soluciones a diversos casos y un acervo histórico automatizado.

A la par de poder mejorar los trámites y servicios, el big data podría ser la mejor métrica, por ejemplo, para lograr medir la cantidad de satisfacción de personas atendidas en las diversas entidades del país, pues el big data podría incluso llevarse al plano de redes sociales y con ello reforzar las estrategias de atención directa, como factor preventivo a ataques infundados y mediatizados, el big data juega papeles benéficos.

Por último, algo que quizá tengamos en nuestras manos como usuarios, pero no logramos comprender es, la Inteligencia

.....
25. Oracle. ¿Qué es el big data?. Recuperado de <https://www.oracle.com/mx/big-data/what-is-big-data.html>

Artificial (IA), que es la capacidad de la máquina para otorgar soluciones con base a algoritmos e identificación de casos particulares, y está presente en nuestros móviles de uso cotidiano. Analicemos como podría tener impacto en las labores gubernamentales.

En algunas dependencias y entidades gubernamentales se cuenta con el uso de chatbots, algoritmos preconfigurados para la atención en chats, los cuales dan respuesta para registrar alguna cita, trámite, responder preguntas, brindar ayuda, eficientando y dejando de lado la parte humana de canalización.

El caso mencionado a raíz de la búsqueda de atención lo ejemplificamos con la Agencia Digital de Innovación Pública (ADIP), quienes implementaron un chatbot para atención remota en sus distintas plataformas.

El chatbot “Victoria” se suma a las diversas herramientas presentadas por el Gobierno de la Ciudad de México para atender la pandemia, entre las que destacan: el servicio de información oficial y diagnóstico sobre COVID-19 al enviar la palabra “covid19” al 51515 vía SMS, por mensaje directo a la cuenta del Gobierno de la Ciudad de México en Facebook, ingresando a la página test.covid19.cdmx.gob.mx o por teléfono al marcar a LOCATEL al 55-5658-1111. Así como el sistema de información sobre disponibilidad hospitalaria en la APP CDMX o en el portal web hospitales.covid19.cdmx.gob.mx²⁶.

La inteligencia artificial sirve para agilizar procesos, simplificándolos, las posibilidades son vastas.

.....

26. CDMX. Lanza Gobierno de Ciudad de México y Facebook chatbot “Victoria” en WhatsApp para informar medidas sobre COVID-19. Recuperado de <https://covid19.cdmx.gob.mx/comunicacion/nota/lanzan-gobierno-de-ciudad-de-mexico-y-facebook-chatbot-victoria-whatsapp-para-informar-medidas-sobre-covid-19>

Implementar IA, en las filas internas de **PRODECON** para ayudar a resolver problemas técnicos para el trabajador podría ser una solución que llevaría matices de concientización y adentrarse a intentar resolver por sí mismo el problema, con una serie de vectores identificados para la resolución por parte del sistema; así como agilizar los sistemas de intercambio de información y prevención ante amenazas digitales o correo no deseado, spam, pues la IA puede servir como un filtro de detección automatizada.

En los portales web, con ayuda de chatbots para la atención al contribuyente, el hecho de poder generar una cita identificando la problemática específica agilizaría y magnificaría los esfuerzos de atención.

Reconocer la necesidad de inversión en tecnologías, es un punto de avance, la meta es adentrarnos para tener un buen uso y eficientar, facilitar, y potenciar cada una de las actividades cotidianas.

Consideraciones Finales



Queda claro que los derechos digitales deben ser un tema relevante para México. Su reconocimiento hoy más que nunca, debe hacerse una realidad y, ese contexto evolutivo, adaptativo, debe llevarse de la mano para la implementación interna en cada una de las dependencias y entidades gubernamentales, pues con ello se podrá buscar homologar un marco legislativo tangible y garante.

Para el caso específico de la Procuraduría de la Defensa del Contribuyente, se debe tener la sagacidad para adaptarse al futuro tecnológico cercano, que permita simplificar tareas cotidianas y maximizar esfuerzos, para mantener siempre un alcance ciudadano pertinente.

Cada miembro de una organización debe comenzar a romper el estereotipo reactivo a las TIC, e impregnarse de los temas de vanguardia que están a la vuelta de la esquina, en el entendido de que esta sociedad informatizada avanza a pasos agigantados.

Las tecnologías como inteligencia artificial, big data y blockchain podrán brindar mayores parámetros de eficiencia y eficacia en distintas dependencias e incluso tareas cotidianas de un usuario común, el despliegue de una mejor y mayor infraestructura para lograr acabar con la brecha digital tanto en poblaciones alejadas, como en entornos ciudadanos que por negación al uso de la tecnología se estancan; la implementación de tales tecnologías deben llevarse de la mano con una colaboración entre diversos sectores, academia, gobierno, empresas y ciudadanía.

Existen muchos temas de atención ante la utilización de TIC en el trabajo y a lo largo de la vida cotidiana, pero debemos

abordarlos con la mejor disposición e instrumentos tecnológicos a nuestro alcance, pues el adaptarse al entorno digital imperante es una necesidad para subsistir y desarrollarse en el día a día.

Bibliografía

Ayuda Ley Protección de Datos. 2018. Derechos Digitales. Recuperado de <https://ayudaleyprotecciondatos.es/2018/10/03/derechos-digitales/>

BID. 2020. COVID-19: Transparencia para asegurar políticas efectivas en momentos de crisis. Recuperado de <https://blogs.iadb.org/administracion-publica/es/covid-19-transparencia-como-un-medio-para-asegurar-la-efectividad-de-las-politicas-en-momentos-de-crisis/>

CEPAL. 2020. Las oportunidades de la digitalización en américa latina frente al covid-19. Recuperado de <https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19.es.pdf>

Cities for Digital Rights. Declaration of Cities Coalition for Digital Rights. Recuperado de https://citiesfordigitalrights.org/assets/Declaration_Cities_for_Digital_Rights.pdf

Consejo de Europa. 2014. Recomendación CM/Rec(2014)6 y exposición de motivos. GUÍA DE LOS DERECHOS HUMANOS PARA LOS USUARIOS DE INTERNET. Recuperado de <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cc3b7>

EUROPOL. 2020. COVID-19: Child sexual exploitation. Recuperado de <https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation>

Gobierno de España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recuperado de <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

Gobierno de México. ¿Cuántos usuarios de internet somos en México? Recuperado de <https://www.gob.mx/sct/articulos/cuantos-usuarios-de-internet-somos-en-mexico>

Gobierno de México. 2013-2018. Estrategia Digital Nacional. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf

Gobierno de México. 2017. Estrategia Nacional de Ciberseguridad. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México. 2018. Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/428335/DDP_Guía_derechos_ARCO_13Dic18.pdf

Gobierno de México. 2018. Historia y logros de la EDN. Recuperado de https://framework-gb.cdn.gob.mx/data/institutos/edn/3dic_publicacion_final_EDN.pdf

Gobierno de México. 2020. INAI. Recuperado de <https://www.gob.mx/sfp/documentos/instituto-nacional-de-transparencia-acceso-a-la-informacion-y-proteccion-de-datos-personales-inai>

Gobierno de México. 2020. Información general. Recuperado de <https://coronavirus.gob.mx/informacion-accesible/>

Gobierno de México. 2020. Positivos estimados al 4 de agosto del 2020. Recuperado de <https://coronavirus.gob.mx/datos/>

Gobierno de México. DOF 04/06/2015. Disposiciones Generales para la implementación, operación y funcionamiento de la Ventanilla Única Nacional. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5395238&fecha=04/06/2015

Gobierno de México. DOF 09/12/2019. Reglamento de la Oficina de la Presidencia de la República. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09/12/2019

Gobierno de México. DOF 14/04/2020. Acuerdo por el que se establecen los Lineamientos para el intercambio de información oficial a través de correo electrónico institucional como medida complementaria de las acciones para el combate de la enfermedad generada por el virus SARS-CoV2 (COVID-19). Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5591878&fecha=17/04/2020

Gobierno de México. DOF 23/04/20. Decreto por el que se establecen las medidas de austeridad que deberán observar las dependencias y entidades de la Administración Pública Federal bajo los criterios que en el mismo se indican. Recuperado de https://dof.gob.mx/nota_detalle.php?codigo=5592205&fecha=23/04/2020

Gobierno de México. DOF 23/07/2018. Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5532585&fecha=23/07/2018

Gobierno de México. DOF 29/01/2016. Decreto por el que se declaran reformadas y derogadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de la reforma política de la Ciudad de México.

Google. Cifras de fallecidos en México por Covid-19 al 11 de agosto del 2020.

Lookingglass Cyber Solutions. 2018. Mexico: Cyber Threat Landscape. Recuperado de https://www.lookingglasscyber.com/wp-content/uploads/2019/03/STRATISS-Cyber_Landscape_Mexico.pdf

Naciones Unidas. Día mundial de las Telecomunicaciones y de la Sociedad de la Información 17 de mayo. Recuperado de <https://www.un.org/es/observances/telecommunication-day>

ONU. Objetivos y metas de desarrollo sostenible. Recuperado de <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>

Oracle. ¿Qué es el big data?. Recuperado de <https://www.oracle.com/mx/big-data/what-is-big-data.html>

Plan Nacional de Desarrollo 2019-2024. DOF 12/07/2019. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019

Sistemius. 2020. El testamento digital en la nueva LOPD. Recuperado de <https://www.sistemius.com/testamento-digital-la-nueva-lopd/>

UNESCO. 2020. Coalición Mundial para la Educación COVID-19. Recuperado de <https://es.unesco.org/covid19/globaleducationcoalition>

UNICEF. 2020. Child rights in the digital age. Recuperado de <https://www.unicef-irc.org/research/child-rights-in-the-digital-age/>

World Economic Forum. 2015. What are your digital rights?. Recuperado de <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/>

Prospectivas de Implementación Tecnológica en la Administración Pública: México

PRODECON

En una reflexión obligada tras los acontecimientos actuales en que vivimos todas las personas del planeta, por el confinamiento al que hemos sido orillados con motivo de la pandemia del virus SARS-Cov-2, conocido también como COVID-19, las actividades económicas, educativas, sociales, culturales y jurídicas que se hacían de forma presencial, han migrado gradualmente al mundo virtual, lo que ha permitido continuar con ciertas acciones que implican el ejercicio de derechos y el cumplimiento de obligaciones por parte de las personas.

En este contexto, el desarrollo de las tecnologías de la información y comunicación, conocidas como TIC, ha sido esencial para que los gobiernos continúen prestando sus servicios a la población de forma remota, a distancia o virtual.

En este estudio **PRODECON** comparte su experiencia en dicho tránsito hacia la virtualidad y la forma en que ha continuado su labor como el *Ombudsperson* fiscal que observa, protege y defiende los derechos de los contribuyentes en México, pero también aprovecha para identificar las oportunidades que existen para mejorar dicho entorno virtual, al abordar temas que inciden de forma directa en la necesidad de que exista legislación que regule los “Derechos Digitales”, tanto en su definición, como en su alcance y contenido.

