



OBLIGACIONES, RECOMENDACIONES Y MEDIDAS A CONSIDERAR EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES ANTE FENÓMENOS METEOROLÓGICOS

Recientemente el Servicio Meteorológico Nacional de México, informó que existe una amenaza de que el huracán Beryl, provoque lluvias intensas en territorio mexicano y que el temporal toque tierra en la península de Yucatán entre la noche de este próximo jueves y la madrugada del viernes; motivo por el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI o Instituto), manifiesta su preocupación por las repercusiones que pudiera tener dicho fenómeno natural en las personas, entidades públicas y privadas que se constituyan como responsables de algún tratamiento de datos personales y población en general, por lo que, considerando que la protección de los datos personales durante cualquier desastre natural, es crucial para preservar la privacidad y seguridad de la ciudadanía, se emiten algunas recomendaciones para el cuidado y debido tratamiento de los datos personales.

Al respecto, es importante tener en cuenta que un fenómeno natural como lo es un huracán, es predecible por lo que las recomendaciones para proteger los datos personales, se pueden advertir desde tres diferentes momentos, a saber, antes, durante y después.

De manera previa a que el huracán toque suelo mexicano, se recomiendan las acciones siguientes:

Por parte de las personas titulares:

- **Realizar copias de seguridad** de tus datos importantes en un lugar seguro y fuera de tu ubicación física. Puedes usar servicios en la nube o discos duros externos;
- **Guardar documentos importantes** (como pasaportes, identificaciones, contratos) en bolsas impermeables o cajas selladas. También puedes escanearlos y almacenar copias digitales.
- **Desconectar dispositivos electrónicos** (teléfonos, computadoras, tabletas) y mantenerlos en un lugar seguro y alejados del agua.
- **Mantener actualizada tu lista de contactos de emergencia**, en la cual incluyas familiares, amigos y servicios de ayuda.
- **Informarse sobre las políticas de privacidad** de las aplicaciones y servicios que utilizas y conoce cómo manejan tus datos personales y qué derechos tienes.

Por parte de los responsables:

- **Elaborar copias de seguridad de las bases y sistemas de tratamiento de datos personales** que tengan en su posesión a efecto de que se mantenga resguardada, para lo que se deberá evaluar si, en el caso particular, resulta conveniente optar por el almacenamiento digital o en su caso identificar ubicaciones físicas seguras fuera del sitio en donde se pre
- **Evaluar los posibles riesgos** asociados que pudieran presentarse relacionados con el desastre natural, con la finalidad de identificar si se cuenta con un plan que permita acciones para mitigarlos, o en caso contrario, elaborar un plan que abarque el ámbito administrativo, físico y técnico para la atención de los riesgos que se presente.
- **Capacitar al personal** que realice un el tratamiento de datos personales para que identifique cuáles serán las acciones que tendrán que realizar en el marco de sus roles y funciones dentro de la organización ante la llegada de un fenómeno natural, con la finalidad de implementar prácticas seguras de manejo de datos y en medidas de seguridad durante emergencias.



Durante permanencia del huracán en territorio nacional:

Por parte de las personas titulares:

- **Identifica tus documentos de identidad más importante** y llévalos contigo si tienes que salir de tu domicilio hacia un lugar de resguardo o ayuda.
- **Limita la información personal que compartes en redes sociales** y evita publicar detalles sobre tu ubicación o planes durante el huracán.
- Si tienes **condiciones médicas importantes**, lleva contigo una tarjeta o pulsera de identificación médica con detalles relevantes.
- **Protege tus documentos y dispositivos** en bolsas impermeables o contenedores sellados y evita dejarlos expuestos al agua o al viento.
- **Utiliza conexiones seguras**, si necesitas acceder a internet para obtener información o comunicarte, utiliza conexiones seguras como redes privadas virtuales (VPN) para proteger tus datos de posibles ataques cibernéticos.
- **Explica a todos los miembros de tu familia** para que comprendan la importancia de proteger la información personal y sepan cómo actuar en caso de emergencia para minimizar riesgos.

Por parte de los responsables:

- **Evitar implementar nuevos tratamientos de datos personales** que no sean necesarios y sin la observancia de los principios y deberes establecidos en la normatividad en materia de datos personales.
- **Mantener comunicación con las autoridades**, inclusive con el Instituto u Organismos Garantes, a fin de tener en cuenta nuevas recomendaciones o medidas a implementar en materia de protección de datos.
- **Avisar a manera de buena práctica** a las personas titulares sobre las medidas de seguridad implementadas y en su caso informarles si derivado de la contingencia que se presenta se hace necesaria la obtención de información personal a efecto de tomar las medidas necesarias para que en estos tratamientos se dé el cumplimiento de las obligaciones en materia de datos personales.
- **Recolectar solo la información necesaria** durante la emergencia y asegurar su eliminación o anonimización cuando ya no sea necesaria.

Después de que el huracán pase por territorio nacional:

Por parte de las personas titulares:

- Tener **cuidado con correos electrónicos o mensajes sospechosos** que ofrezcan apoyos y ayuda para damnificados por el huracán, pues pueden intentar tus datos personales, por lo que deberás verificar la autenticidad de las comunicaciones antes de proporcionar información.
- **No compartir información personal innecesariamente** evitar compartir información personal en redes sociales u otras plataformas públicas, especialmente en situaciones de crisis donde los estafadores pueden aprovecharse.
- **Consultar fuentes oficiales** y verificar que la información y las ofertas de ayuda provengan de sitios confiables, como páginas web gubernamentales y organizaciones reconocidas.

Por parte de los responsables:

- Ante cualquier incidente o vulneración de seguridad, deberá notificar sin dilación alguna a los titulares de los datos personales, así como al Instituto.



- Facilita el ejercicio de derechos ARCO de las personas afectadas por el fenómeno natural, deberá identificarse la procedencia de estos derechos que requieran las personas afectadas y damnificadas frente a la contingencia.
- Priorizar la atención de los documentos y/o archivos siniestrados que contengan datos personales y datos personales sensibles, como nombres, domicilios, números de identificación, datos de salud, etc., para evitar su uso indebido o su divulgación no autorizada.
- La protección de datos personales puede salvar vidas, por ello deberá cuidarse que exista un trato digno y sin discriminación a las personas afectadas en función de su origen étnico o racial, estado de salud, situación socioeconómica o edad, teniendo especial cuidado con el tratamiento de los datos personales de las personas en estado de vulnerabilidad especial y menores de edad.
- En la difusión que se realice en redes sociales y medios de comunicación, deberá cuidarse que el tratamiento de los datos personales sea proporcional y mínimo para cumplir con las finalidades que se persigan en atención a la localización de familiares, centros hospitalarios y de salud, zonas de riesgo, albergues, entrega de apoyos públicos y privados.
- Las personas afectadas deberán procurar contar con documentos de identidad y en caso de que esto no sea posible, deberá procurarse que tengan la oportunidad de contactar con sus familiares o amigos.
- Deberá cuidarse que las autoridades y personas u organizaciones voluntarias se encuentren identificadas a través de uniformes o signos distintivos, a fin de evitar que los datos personales que se entreguen puedan ser utilizados para fraudes y extorsiones.
- En el caso de personas afectadas de origen extranjero, deberá proporcionarse la asistencia consular que corresponda previa autorización y bajo su más estricta elección.
- No deberían condicionarse la identidad o calidad migratoria de las personas para proporcionar cualquier tipo de servicio que les permita canalizarlos ante las autoridades respectivas.
- Deberá procurarse que el tratamiento de datos personales que realizan todas las personas que intervengan para asistir a personas damnificadas o afectadas, establezca las medidas de seguridad necesaria que permitan cuidar la confidencialidad, integridad y disponibilidad de los datos personales, a fin de evitar su pérdida, destrucción, divulgación, uso o acceso no autorizado, extravío, o cualquier otro similar.
- Tratándose del uso de datos patrimoniales o financieros que requieran utilizar las personas afectadas, se remitirá únicamente a personas y canales autorizados por las instituciones bancarias.
- Implementar medidas compensatorias cuando proceda, a fin de que las personas titulares conozcan el Aviso de Privacidad y la identidad de quiénes utilizaron sus datos personales.
- Informar sin demora al titular, y según corresponda, al Instituto y al Organismo garante de las Entidades Federativas dentro de los plazos establecidos, de las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, para que los titulares afectados puedan tomar las medidas adecuadas para la defensa de sus derechos.
- Implementar las acciones correctivas necesarias para ajustar las medidas de seguridad y el tratamiento de los datos personales si fuera el caso a fin de prevenir que la vulneración se vuelva a producir.