“La protección de datos personales en la pandemia COVID-19”

Mtro. Jonathan Mendoza Iserte
Secretario de Protección de Datos Personales

El mundo después del Coronavirus

“This storm will pass. But the choices we make now could change our lives for years to come”.

Esta tormenta pasará. Pero las decisiones que hagamos ahora podrían cambiar nuestras vidas en los próximos años.

Yuval Noah Harari
Financial times
19 de Marzo

“You could, of course, make the case for biometric surveillance as a temporary measure taken during a state of emergency. It would go away once the emergency is over. But temporary measures have a nasty habit of outlasting emergencies, especially as there is always a new emergency lurking on the horizon”.

Podría, por supuesto, defender la vigilancia biométrica como una medida temporal tomada durante un estado de emergencia. Se iría una vez que termine la emergencia. Pero las medidas temporales tienen el desagradable hábito de superar las emergencias, especialmente porque siempre hay una nueva emergencia al acecho en el horizonte.

Yuval Noah Harari

Wojciech Wiewiórowski
Supervisor Europeo de Protección de Datos

"La protección de datos no es un obstáculo para combatir la pandemia. Las aplicaciones de rastreo de contactos deberían funcionar temporalmente, con un propósito específico y minimizando los datos. Esto es clave para generar confianza entre las personas, aumentar la eficiencia y proteger los derechos fundamentales". WW

EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

OEA
Más derechos para más gente

CIDH
Comisión Interamericana de Derechos Humanos

35. Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia.

- Consentimiento.
- Fin limitado de combatir la pandemia.
- Las personas afectadas conservarán el derecho a cancelación de sus datos personales.

36. Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales.

El acceso a la información veraz y fiable, así como a internet, es esencial. Deben disponerse las medidas adecuadas para que el uso de tecnología de vigilancia para monitorear y rastrear la propagación del coronavirus COVID19, sea limitado y proporcional a las necesidades sanitarias y no implique una injerencia desmedida y lesiva para la privacidad, la protección de datos personales, y a la observancia del principio general de no discriminación.

Comunicado

Corte Interamericana de Derechos Humanos

Corte IDH_CP-27/2020 Español

Si tiene problemas para visualizar este mensaje haga clic AQUÍ

Corte IDH

Protegiendo Derechos

COVID-19 Y DERECHOS HUMANOS: LOS PROBLEMAS Y DESAFÍOS DEBEN SER ABORDADOS CON PERSPECTIVA DE DERECHOS HUMANOS Y RESPETANDO LAS OBLIGACIONES INTERNACIONALES

San José, Costa Rica, 14 de abril de 2020. La Corte Interamericana de Derechos Humanos ha adoptado, el pasado jueves 9 de abril de 2020, una Declaración titulada "COVID-19 y Derechos Humanos: Los problemas y desafíos deben ser abordados con perspectiva de Derechos Humanos y respetando las obligaciones internacionales".

Eduardo Ferrer Mac-Gregor Poisot
Juez de la Corte IDH

"Seminario: Restricciones y suspensión de derechos y sus consecuencias en el marco del COVID-19"

San José, Costa Rica, 5 de junio de 2020.

El Juez Eduardo Ferrer Mac-Gregor en concordancia con la Declaración 1/2020, sobre Covid-19 y Derechos Humanos, señaló que las respuestas de los Estados tienen que ser abordadas desde una perspectiva de los derechos humanos. Las medidas de emergencia no deben servir de pretexto para abusos y vulneraciones de derechos humanos".

Además, señaló que, si bien la Corte no ha enfrentado a través de su jurisprudencia una situación similar a esta pandemia, "en sus más de cuatro décadas de existencia, el Tribunal ha establecido criterios específicos que deben cumplirse cuando se trate tanto de una suspensión como de una restricción o afectación de derechos".

Desde la CIDH se ha trabajado en el establecimiento de estándares de protección diferenciados que determinen las obligaciones particulares de los Estados con respecto a los grupos en mayor situación de vulnerabilidad, como son:

- Personas en situación de pobreza sin acceso a salud, alimentación y vivienda
- Mujeres y niñas que enfrentan violencia al interior de los hogares
- Personas mayores discriminadas en el acceso a la salud
- Niñas y niños cuyo derecho a la educación se ve truncado
- Personas que han sido privadas de la libertad
- Migrantes, refugiados y desplazados internos

En el marco de esta pandemia, 10 Estados que han ratificado la Convención Americana han declarado Estados de emergencia nacional: Argentina, Bolivia, Chile, Colombia, El Salvador, Ecuador, Guatemala, Honduras, Panamá y Perú.

Seguimiento y rastreo del COVID: Protección de la privacidad y los datos al utilizar aplicaciones y biometría

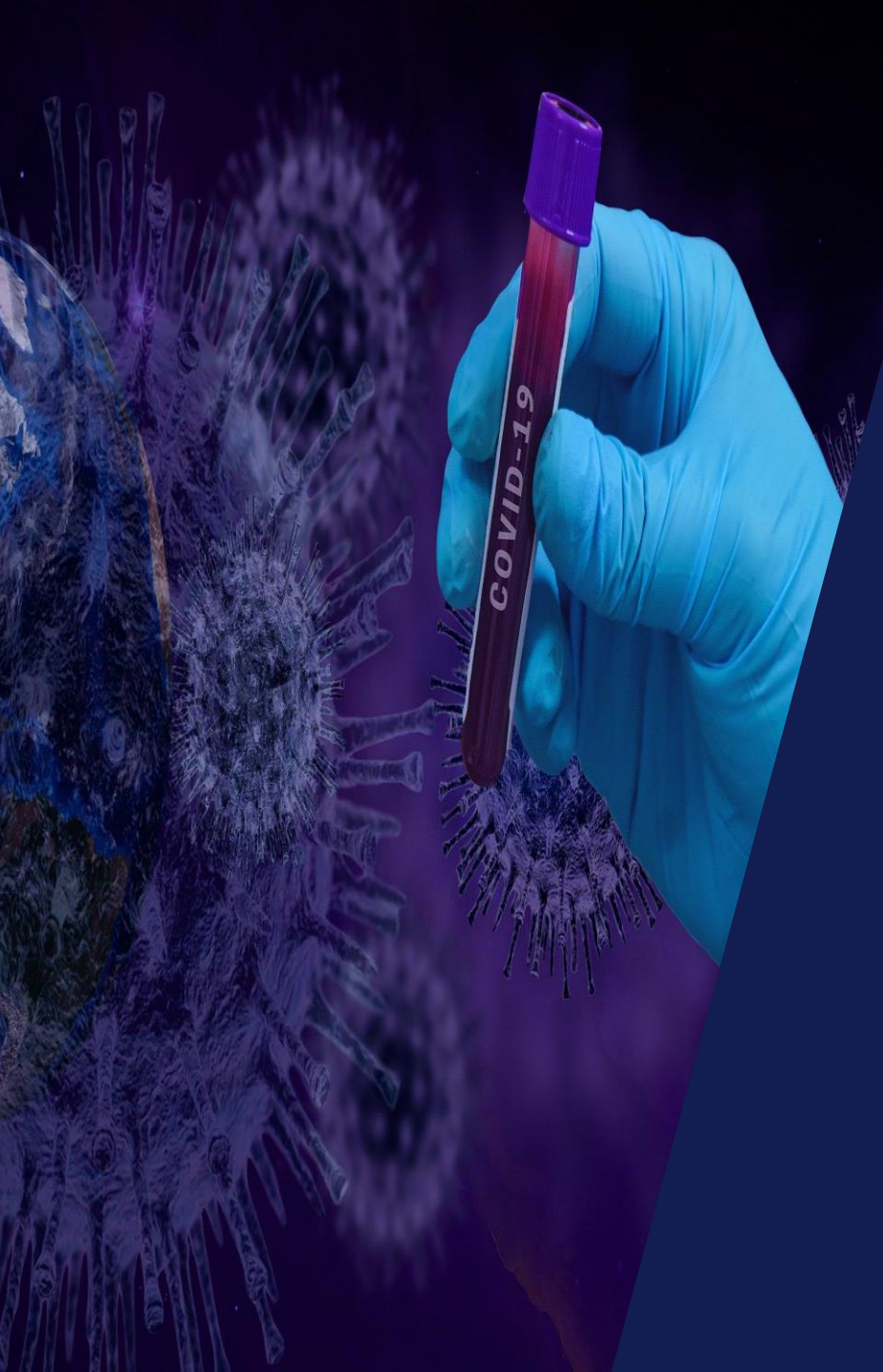
La importancia de la colaboración gubernamental con el sector de telecomunicaciones para acceder a datos GPS, rastreando así población objetivo y contener el virus, esto, a través de apps referentes al ecosistema de salud en observancia al COVID-19.

Garantizando la privacidad de los datos mientras luchamos contra el COVID-19

Ensuring data privacy as we battle COVID-19 EN

Usar la inteligencia artificial para ayudar a combatir el COVID-19

Using artificial intelligence to help combat COVID-19 EN



Tratamiento de datos personales durante la emergencia sanitaria por COVID-19

La información obtenida o generada en el ámbito de la salud, da cuenta de rasgos íntimos de las personas, como el historial médico, del que se pueden desprender padecimientos, pasados y presentes; tratamientos recibidos, alergias, información genética, adicciones, información psicológica de la que se puedan obtener trastornos mentales o bien vida sexual. La pérdida, comunicación o transferencia no autorizada de esta información, pone en riesgo la integridad de los titulares de los datos, exponiéndolos a actos discriminatorios o de segregación.

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

La tecnología provee de oportunidades valiosas para potenciar esfuerzos encaminados al desarrollo social. Pero si la tecnología se implementa sin controles claros esta potencia puede devenir en la instrumentalización de las capacidades de recopilación de datos, identificación o incluso diseminación de información con fines que distan del respeto a los derechos humanos y se acercan más a formas de control social.

En esa vaguedad es donde se instaura la posibilidad de que estas medidas excepcionales no solamente se normalicen, sino también sean usadas de forma abusiva en detrimento de los derechos humanos para fortalecer mecanismos de vigilancia y control social.

Jessica Matus
Directora y fundadora de Datos Protegidos (Chile)

"Aplicaciones de rastreo de proximidad COVID-19: estándares de protección de datos y Privacidad por Diseño"

Tanto la privacidad como la salud son derechos fundamentales, y en los marcos regulatorios existen fórmulas para la protección de uno sin detrimento del otro. En este sentido, existen formas de trabajar bajo estándares capaces de resguardar la confidencialidad y seguridad de la información, al mismo tiempo que se implementan soluciones tecnológicas para complementar medidas de las autoridades que permitan contribuir a la situación actual de crisis sanitaria.


Covid - 19 Mx
2-abr-2020
Alerta Honduras
23-mar-2020
Alerta Guate
24-mar-2020
Covid19Tracker
24-mar-2020
CoronApp
15-abr-2020
Coronavirus SUS
7-abr-2020
Salud Ec
25-mar-2020
Perú en tus manos
7-may-2020
Bolivia Segura
9-may-2020
Vico
30 -may-2020
Coronavirus UY
20-mar-2020
CoronApp
16-abr-2020
CuidAr
27-abr.2020
Mapa latinoamericano de Apps Covid-19

Aplicación móvil, creada por la firma salvadoreña *Hardmode Interactive*.

La aplicación revela al usuario un panorama sobre todo el territorio nacional. Rastrea, documenta, muestra fotografías y detalles de los alrededores del domicilio del usuario y la situación de riesgo de los destinos que el sujeto va a visitar o visitó.

La aplicación queda en segundo plano, es decir que funciona pese a que se utilicen otras apps en simultáneo y cada cierto tiempo va registrando la ubicación y las coordenadas del usuario automáticamente.

Al 29 de marzo, no contaba con el apoyo del Gobierno.

Su desarrollo más reciente es la aplicación *Covid19 Tracker Med*.

Esta aplicación está hecha para ayudar a los médicos a encontrar los nexos epidemiológicos.

Ofrece la opción de crear perfiles de pacientes que una vez identificados como caso sospechoso de contagio se registran en esta aplicación.

La aplicación solicita nombre, correo electrónico, DUI y dirección.

En la página en la que se puede descargar la aplicación no hay referencias sobre el tratamiento de los datos personales.

Manuela Battaglini
Aboga experta en ética de datos

“Marco socio-tecnológico para las aplicaciones de rastreo de contagios de Covid-19”

Las aplicaciones de rastreo de contactos son un claro ejemplo de ética digital y deberían ser analizadas desde su diseño para saber si están alineadas con las necesidades de los individuos, respetando sus derechos humanos, garantizando la transparencia en todos sus procedimientos mediante el uso de tecnologías no invasivas, resguardas por el Estado y contemplando cláusulas de expiración y borrado de la información para garantizar y dar confianza a la ciudadanía.


Expediente clínico y datos personales

Ley General de Salud y Expediente Clínico Electrónico (ECE)

- En México, la Ley General de Salud hace referencia, de forma somera, al expediente clínico en la aplicación de los procedimientos diagnósticos y terapéuticos.

- Del mismo modo, lo señala como el documento en el cual se deja constancia de los procedimientos o actividades que el médico realiza.

- También se habla de la integración de expedientes clínicos como un elemento de acreditación de la calidad de los servicios médicos.

Expediente Clínico

El INAI ha resuelto que el derecho de acceso al expediente clínico es un derecho de vital importancia porque permite el ejercicio de otros derechos humanos como el derecho a la salud de las personas.

La titularidad de los datos personales contenidos en un expediente clínico corresponde al paciente, quien puede ejercer sus derechos con relación a la información personal proporcionada como solicitar una copia del mismo y a la confidencialidad de sus datos personales.

Procedimiento en el tratamiento de datos personales

Sector PRIVADO

- Procedimiento de investigación
- Procedimiento de verificación
- Procedimiento de protección de derechos
- Procedimiento de imposición de sanciones

Sector PÚBLICO

- Procedimiento de investigación
- Procedimiento de verificación
- Recurso de Revisión
- Procedimiento de imposición de sanciones / Órgano Interno de Control

PROTECCIÓN DE DATOS PERSONALES
durante el trabajo a distancia

inai

Dispositivos móviles (tabletas electrónicas, *smartphones*, laptops)

- Instalar medidas de seguridad que protejan a los dispositivos móviles de cualquier *software* malicioso que pueda comprometer la información y datos personales que éstos almacenan.

- Asegurar que los dispositivos que se utilicen para tratar datos personales o información de la organización cuenten con las últimas actualizaciones instaladas.

- Verificar que el entorno donde se utilicen los dispositivos móviles sea seguro, para evitar su pérdida o extravío, así como la exposición de datos personales o información a personas no autorizadas.

- Establecer medidas para bloquear el acceso a los dispositivos en donde se realizará el tratamiento de datos personales o información, a través de un código o patrón o huella.

- Usar medidas para controlar el acceso a los dispositivos, aplicaciones o servicios, tales como contraseñas robustas, autenticación de múltiples factores y/o cifrado para restringir el acceso al dispositivo y reducir el riesgo de que se comprometa la seguridad de los datos personales o información.

- Implementar medidas para el borrado remoto de dispositivos en caso de pérdida, robo o extravío.

Personal

- Concientizar al personal sobre la responsabilidad de proteger la integridad, confidencialidad y disponibilidad de la información y datos personales que tratarán para continuar con sus actividades en la modalidad de trabajo a distancia.

- Cumplir con las medidas de seguridad físicas y técnicas establecidas por la organización, para la protección de la información y datos personales.

Acceso a la red y servicios de nube:

- Utilizar los servicios de nube y las redes de confianza de la organización.

- Cumplir con las políticas y procedimientos sobre acceso a la red, servicios de nube, usuarios, contraseñas, intercambio y respaldo de información.

- Usar un canal seguro siempre que se utilice una red pública para conectarse, por ejemplo, una VPN (Red Privada Virtual).

- En caso de requerir acceso a la red de la organización, para operar sistemas de información, administrar recursos tecnológicos de forma remota o consultar información de la intranet, se sugiere utilizar una VPN.

- Realizar una revisión física para verificar que los elementos de red funcionen correctamente (modem, cableado, corriente eléctrica, intensidad de la señal).

Correo electrónico:

- Cumplir con las políticas de la organización relacionadas con el uso de correo electrónico.

- Usar las cuentas de correo electrónico de trabajo en lugar de cuentas personales para correos electrónicos relacionados con actividades laborales que traten datos personales.

- Si es estrictamente necesario utilizar cuentas de correo electrónico personal para enviar datos personales o información confidencial adjunta, ésta deberá estar cifrada.

- Evitar incluir datos personales o información confidencial en el asunto del correo electrónico.

- Antes de enviar un correo electrónico verificar que la dirección del destinatario sea correcta, especialmente en casos donde se envíen datos personales y/o sensibles.

- Verificar que el entorno donde se utilice el correo electrónico sea seguro, para evitar que personas no autorizadas tengan acceso a datos personales o información.

TRATAMIENTO DE DATOS PERSONALES **EN NOTAS PERIODÍSTICAS Y MEDIOS DE COMUNICACIÓN**

CORONA**VIRUS** COVID-19

Los datos personales concernientes al estado de salud de las personas vinculados con el tratamiento médico que reciben en las instancias de salud en los casos de COVID-19, no pueden divulgarse asociados al nombre del paciente o información que los haga identificables.

Los medios de comunicación se consideran sujetos regulados (sector privado), o bien, sujetos obligados (sector público) en la medida en que llevan a cabo el tratamiento de datos personales para el desarrollo de sus actividades; lo que implica que el ejercicio del derecho fundamental a la libertad de expresión que realizan de conformidad con la naturaleza jurídica pública o privada que revistan, debe ajustarse a un ejercicio ético y sujeto a responsabilidades ulteriores

Los responsables en el tratamiento de datos personales, incluyendo los de salud, deben cumplir el **principio de proporcionalidad**, lo que implica la obligación de que su uso resulte necesario, adecuado y relevante en relación con las finalidades para las cuales se hayan obtenido, debiendo realizarse esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios en relación con casos de COVID-19.

Los responsables deben garantizar el deber de **confidencialidad** respecto de los datos personales y datos personales sensibles de cualquier titular a los que tengan acceso, relacionado con casos de COVID-19, para evitar daño o discriminación de la persona afectada.

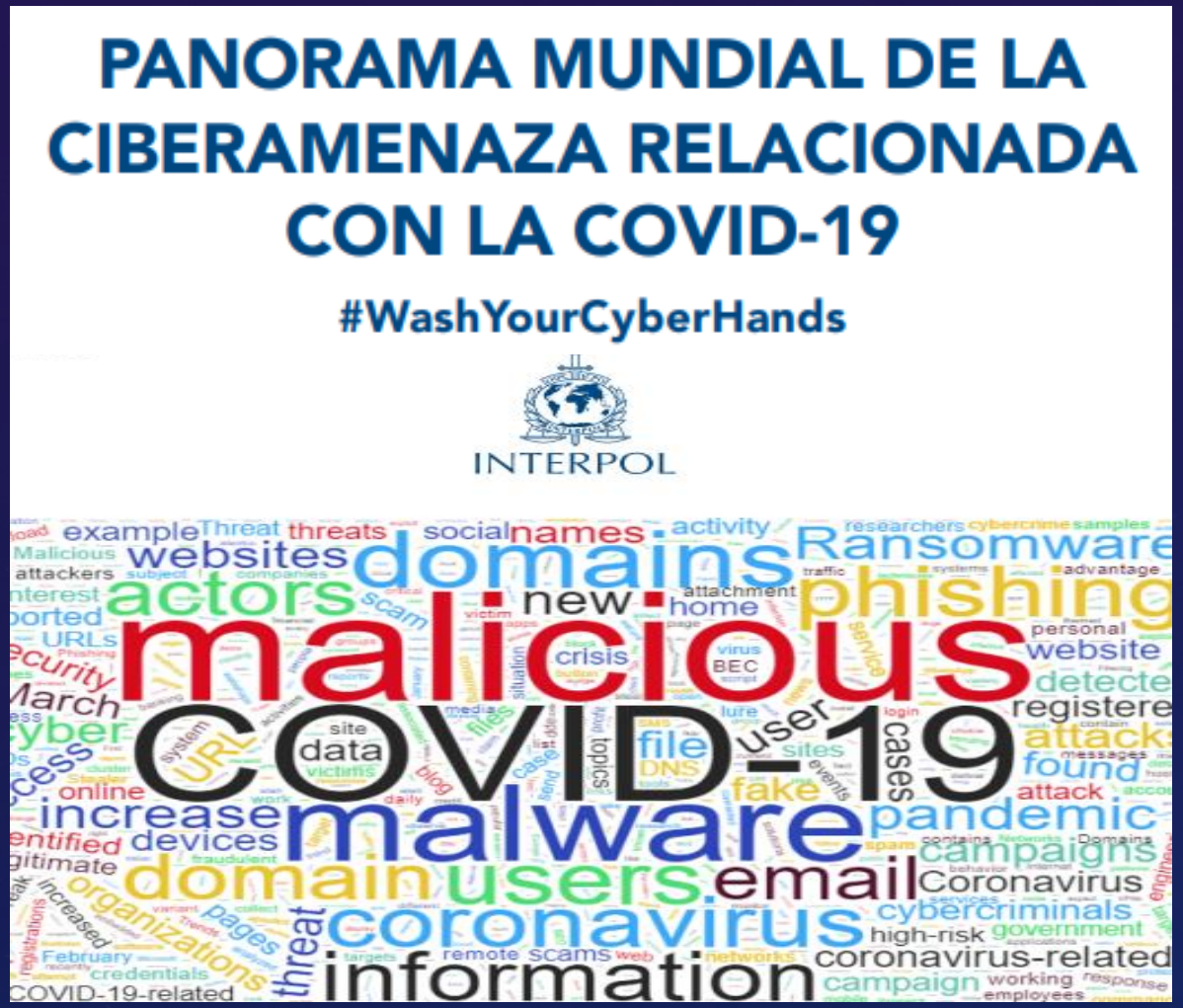
No se puede divulgar la identidad de los titulares sospechosos o afectados por el COVID-19, evitando la obtención y tratamiento de información y datos personales que resulten innecesarios, no pertinentes o excesivos.

El tratamiento de los datos personales obtenidos con el fin de brindar información a la sociedad en ejercicio del derecho a la libertad de expresión debe ajustarse a las leyes de la materia (LFPDPPP y LGPDPPSO), sin que puedan utilizarse para propósitos que puedan dar origen a discriminación o conlleve un riesgo grave para sus titulares.

LGPDPPSO -Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
LFPDPPP -Ley Federal de Protección de Datos Personales en Posesión de los Particulares

inai

Otras amenazas



- Dominios malignos
- Estafas en línea y *phishing*
- Malware para recolección de datos
- Malware obstructivos
- Vulnerabilidad del trabajo a domicilio

¡NO PONGAS EN RIESGO TUS DATOS PERSONALES!

FRAUDES MÁS UTILIZADOS EN LA EMERGENCIA SANITARIA POR COVID-19

#TusDatosValen
#INAITeDefiende

MENSAJES INFORMATIVOS CON ENLACES MALICIOSOS

Remiten a información o recomendaciones sobre COVID-19, buscan la atención del usuario para que visite sitios maliciosos que solicitan información personal.

RANSOMWARE

Archivos adjuntos de correo electrónico o mensaje de texto que contienen un programa malicioso que puede infectar, cifrar o tomar el control de nuestros equipos, y afectar la confidencialidad y disponibilidad de nuestros datos personales y de la información almacenada.

MENSAJES DE SOLIDARIDAD

Aprovechan la situación de emergencia sanitaria para engañar y solicitar apoyo destinado al personal de salud. Algunos piden datos personales o donaciones económicas.

MENSAJES *PHISHING*

Comparten la dirección electrónica de un sitio que suplanta la identidad de otro conocido o de interés del usuario. A través de este engaño, el atacante roba la información o datos personales ingresados por la víctima en el sitio falso.

MENSAJES *SMISHING*

Mensajes SMS que suplantan la identidad de una institución oficial, con la finalidad de compartir un enlace en el que solicitan datos personales.

BENEFICIOS DE PROGRAMAS SOCIALES

Mensajes que suplantan la identidad de instituciones públicas y ofrecen apoyo económico, a través de supuestos programas sociales, para lo cual solicitan datos personales y en algunos casos dinero.

OFERTAS DE TRABAJO

Mensajes que comparten falsas ofertas de empleo y que, para registrarse en las supuestas listas de vacantes, solicitan datos personales.

SOPORTE TÉCNICO FRAUDULENTO

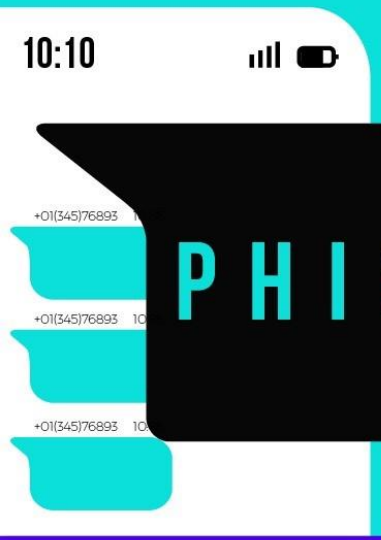
Servicios falsos a través de llamadas o mensajes que aprovechan la situación de trabajo a distancia para obtener datos personales del usuario, incluyendo sus contraseñas.

SERVICIOS GRATUITOS

Mensajes falsos que ofrecen promociones, descuentos o cupones para tener acceso gratuito a servicios de entretenimiento y que, para hacerlos válidos, solicitan datos personales.

Fuente: https://www.osi.es/es/actualidad/blog/2020/03/27/top-10-fraudes-que-utilizan-covid-19-para-enganar-los-usuarios

ANTES DE PROPORCIONAR TUS DATOS PERSONALES ASEGÚRATE DE



PHISHING

PÁGINAS WEB

1. REVISAR SI CUENTAN CON AVISO DE PRIVACIDAD
2. TECLEAR LA DIRECCIÓN DEL SITIO DIRECTAMENTE
3. PRESTAR ATENCIÓN EN LA REDACCIÓN, FALTAS DE ORTOGRAFÍA O SIGNOS EXTRAÑOS DE LOS SITIOS Y MENSAJES ON LINE
4. CONFIGURAR LOS FILTROS DE CORREO NO DESEADO O FRAUDULENTO
5. EVITAR DESCARGAR ARCHIVOS DE FUENTES NO CONFIABLES O REMITENTES DESCONOCIDOS
6. REVISAR DE FORMA PERIÓDICA TUS ESTADOS DE CUENTA BANCARIOS Y DEPARTAMENTALES

NOTA: ACTUALIZA PERIODICAMENTE TUS NAVEGADORES

WIFI GRATUITO

1. EVITAR UTILIZAR REDES PÚBLICAS Y/O INGRESAR A SITIOS FINANCIEROS
2. EVITAR REALIZAR TRANSACCIONES FINANCIERAS O COMPRAS EN PÁGINAS DE COMERCIO ELECTRÓNICO

LLAMADAS TELEFÓNICAS

GUARDAR LA CALMA Y NO DAR INFORMACIÓN CONFIDENCIAL SI RECIBES LLAMADAS ANUNCIADO QUE ERES GANADOR DE ALGÚN PREMIO

EN CASO DE HABER SIDO VÍCTIMA DE PHISHING, RECOPILA TODA LA INFORMACIÓN QUE PUEDA SERVIR COMO EVIDENCIA DEL ENGAÑO Y CONTACTA DE FORMA INMEDIATA A LA ENTIDAD, EMPRESA O INSTITUCIÓN QUE CORRESPONDA.

#LOTIENESQUESABER

Telinai
8008354324

CUIDA CON QUIÉN COMPARTES TU INFORMACIÓN !

Para proteger tus datos personales y evitar ser víctima de fraude, revisa con quién compartes tu información personal.

Ante la emergencia sanitaria generada por COVID-19, existen personas o sitios de Internet que suplantan la identidad de instituciones o empresas para ofrecer supuestos beneficios de programas sociales o promociones que, mediante el engaño, buscan obtener información personal y/o dinero.

#TusDatosValen

INAImx INAImexico inai_mx inaimexico

Posibles consecuencias:

· Pérdidas financieras.

· Fraude.

· Uso no autorizado de cuentas y/o datos personales.

Formas en las que se puede presentar:

· Utilización de imagen o nombre de alguna institución pública o privada conocida.

· Por vía telefónica, a través de un correo electrónico o mensaje de texto al teléfono móvil, en donde se envían enlaces con la falsa promoción.

· Publicaciones engañosas a través de perfiles de redes sociales.

· Llamadas telefónicas.

· Documentos enviados al domicilio de la posible víctima.

inai

Objetivo

Datos Personales Seguros COVID-19 es un micrositio desarrollado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) para brindar información clara y precisa a los titulares sobre el derecho a la protección de sus datos personales que, en su caso, serán tratados en instituciones públicas o privadas a fin de otorgarles el diagnóstico, atención y seguimiento sobre **Coronavirus, COVID-19**. Así como proporcionar recomendaciones para los responsables y encargados del Sector Público y Privado, sobre el adecuado tratamiento de datos personales que deberán realizar en las diversas actividades requeridas para la atención de casos de COVID-19, de forma que se cumpla con los principios, deberes y obligaciones que el marco legal en materia de protección de datos personales establece.

El micrositio compartirá los esfuerzos realizados por las diferentes agencias de protección de datos a nivel internacional para promover medidas, recomendaciones y atención de dudas relacionadas con el tratamiento de datos personales de casos de COVID-19.

¡Gracias!

Mtro. Jonathan Mendoza Iserte

Secretario de Protección de Datos Personales

@JonnhyMendoza