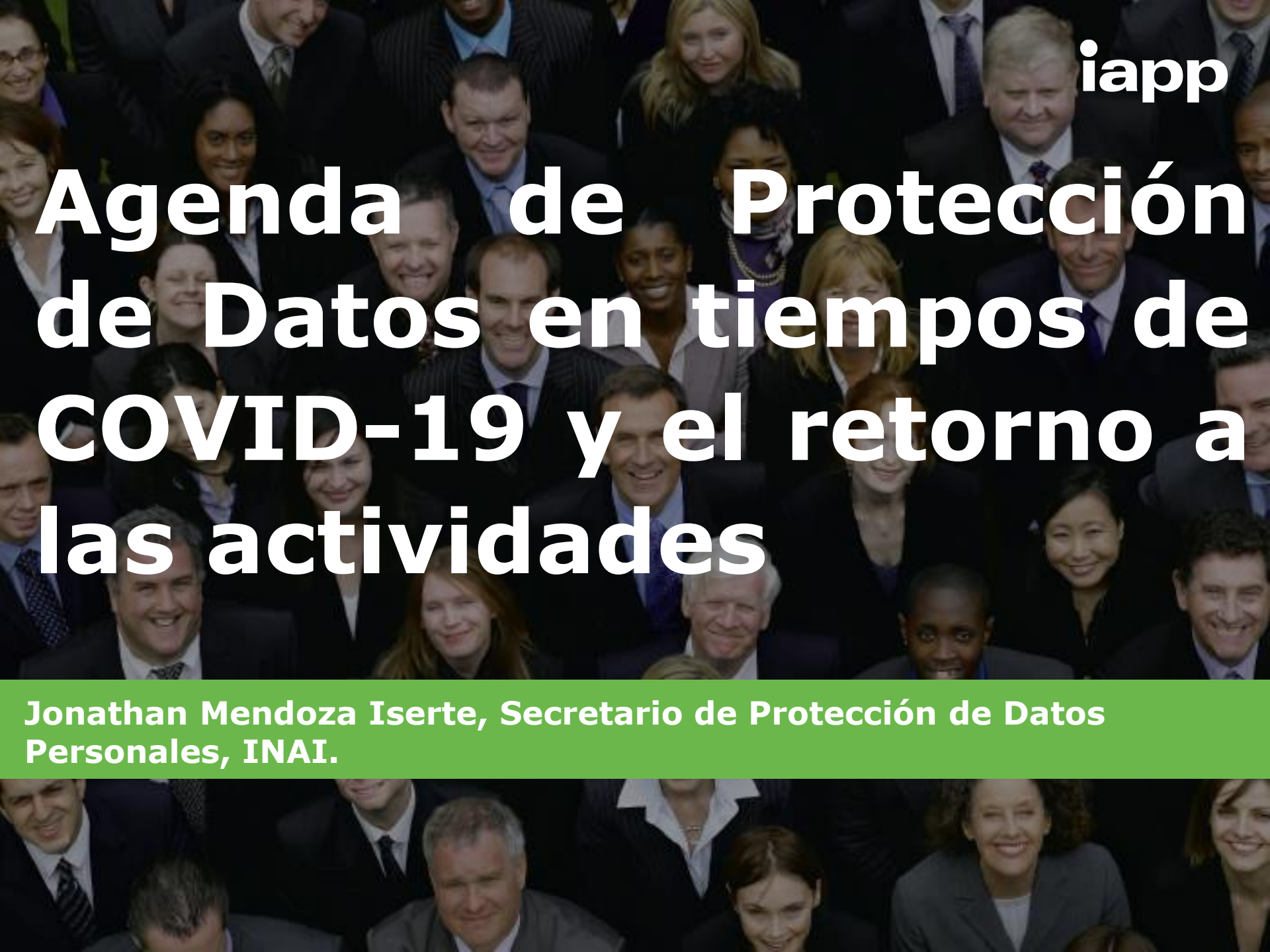
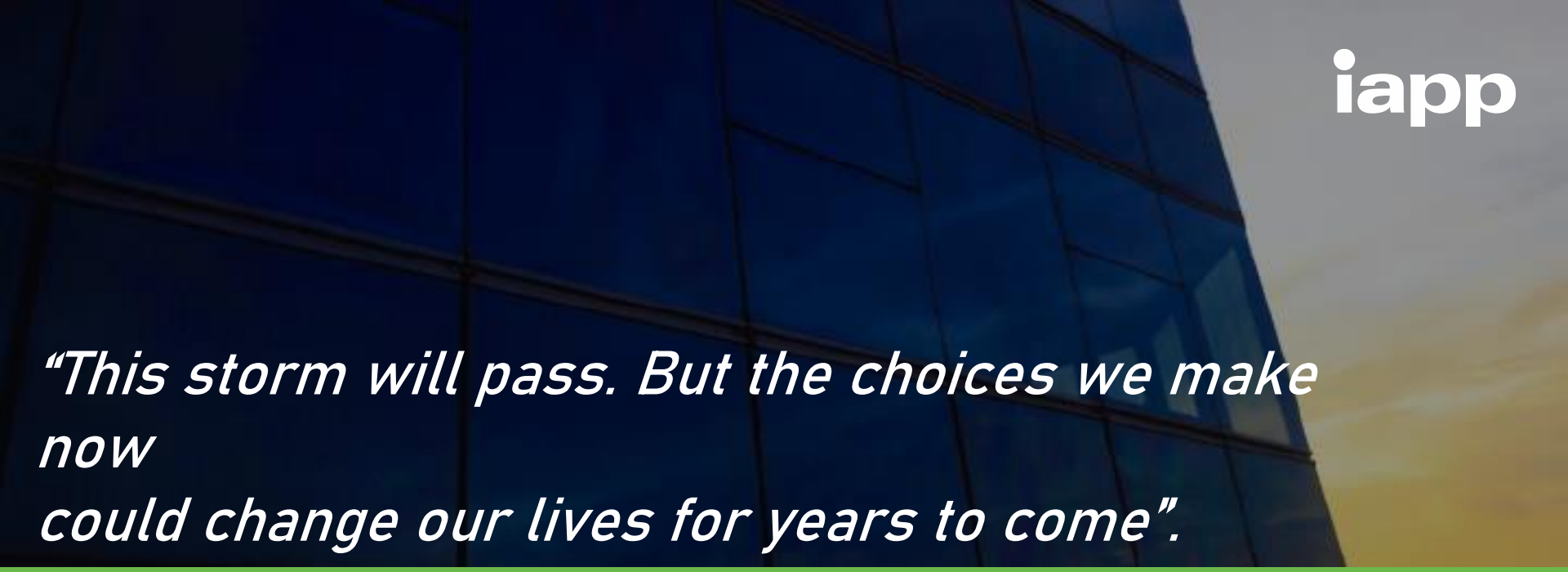


Agenda de Protección de Datos en tiempos de COVID-19 y el retorno a las actividades

Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales, INAI.



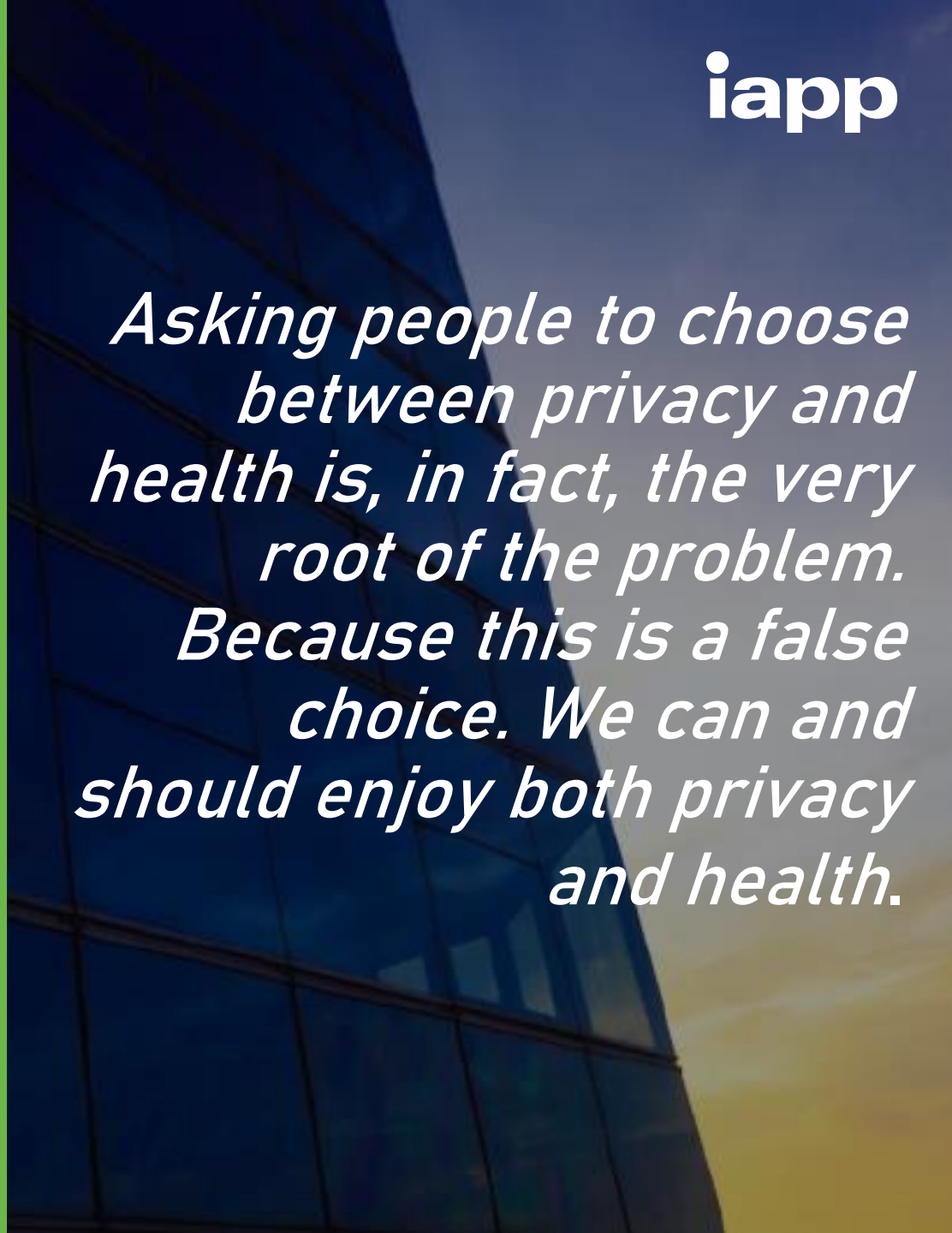
“This storm will pass. But the choices we make now
could change our lives for years to come”.

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

Pedirle a la gente que elija entre privacidad y salud es, de hecho, la raíz del problema. Porque esta es una elección falsa. Podemos y debemos disfrutar tanto de la privacidad como de la salud.

Yuval Noah Harari.



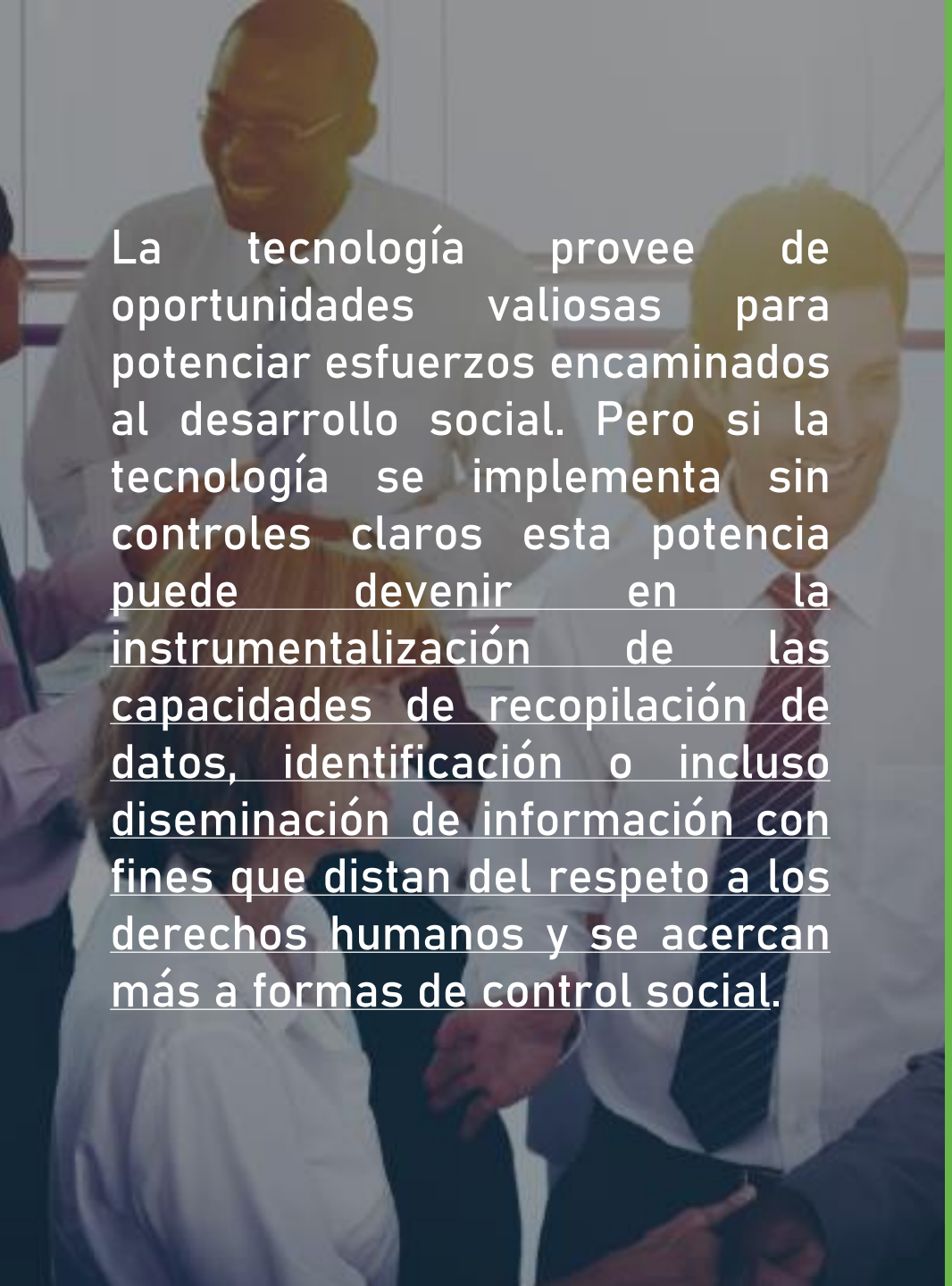
Wojciech Wiewiórowski
Supervisor Europeo de Protección de Datos

"Carrying the torch in times of darkness"

La "nueva normalidad" no debe ceder a la erosión permanente de los derechos por los que hemos luchado tanto y tan difícil ha sido promover. Las normas de protección de datos de la UE deben ser parte del camino de la UE hacia la recuperación.

(EDPS – Abril 30, 2020).

Las legislaciones de protección de datos personales y privacidad en la lucha contra la pandemia COVID-19, NO son un obstáculo, sino un soporte del bienestar y salud.



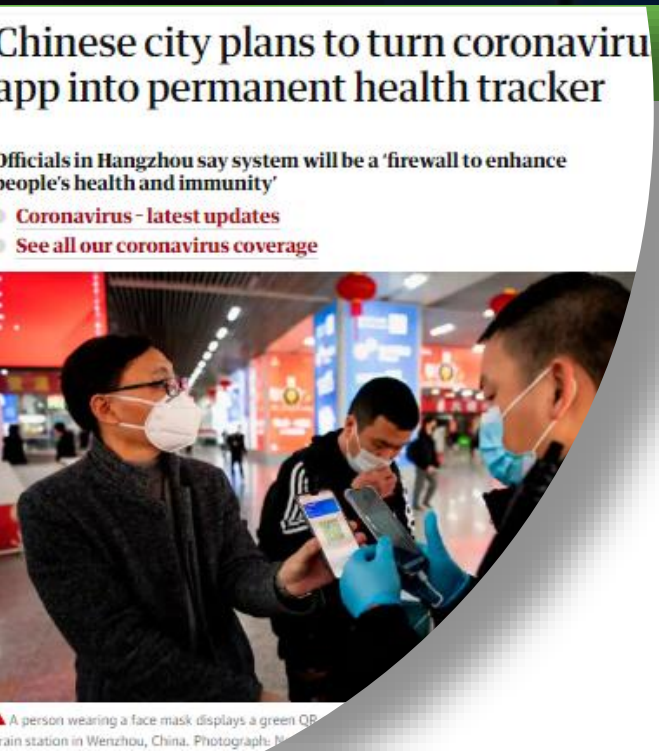
La tecnología provee de oportunidades valiosas para potenciar esfuerzos encaminados al desarrollo social. Pero si la tecnología se implementa sin controles claros esta potencia puede devenir en la instrumentalización de las capacidades de recopilación de datos, identificación o incluso diseminación de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

iapp

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.

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

De acuerdo con una nota publicada por The Guardian (26 de mayo) las autoridades de la Ciudad de Hangzhou buscarán lanzar una versión más amplia de (Health Check) la app de seguimiento utilizada como parte de la respuesta al COVID-19 AHORA para controlar la salud general de las personas.


Chinese city plans to turn coronaviru
app into permanent health tracker

Officials in Hangzhou say system will be a 'firewall to enhance people's health and immunity'

Coronavirus - latest updates

See all our coronavirus coverage

A person wearing a face mask displays a green QR
rain station in Wenzhou, China. Photograph:

En la aplicación propuesta, el estado de SALUD de una persona se codificará por colores y se puntuará HASTA 100 tomando en cuenta: los registros médicos, los resultados de las pruebas físicas, los niveles de actividad y otras opciones de estilo de vida, como fumar.

Privacidad por diseño: una respuesta a una falsa dicotomía

Jessica Matus.

29 de mayo, 2020.

Privacidad y salud son derechos fundamentales, y en marcos regulatorios hay fórmulas para la protección de uno sin perjuicio del otro, que no están suspendidas por la pandemia. En la aplicación de tecnología, en particular, una medida que la sociedad adoptará postetapa de confinamiento es el rastreo de contactos, hoy denominado notificación de exposición.

iapp

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

CIDH
Comisión Interamericana de Derechos Humanos

OEA
Más derechos para más gente

iapp

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.

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".

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.

Acceso a la información: ese acceso comprende el derecho de solicitar, recibir y difundir información e ideas acerca de las cuestiones relacionadas con la salud. Con todo, el acceso a la información no debe menoscabar el derecho de que los datos personales relativos a la salud sean tratados con confidencialidad.

Retorno a las actividades

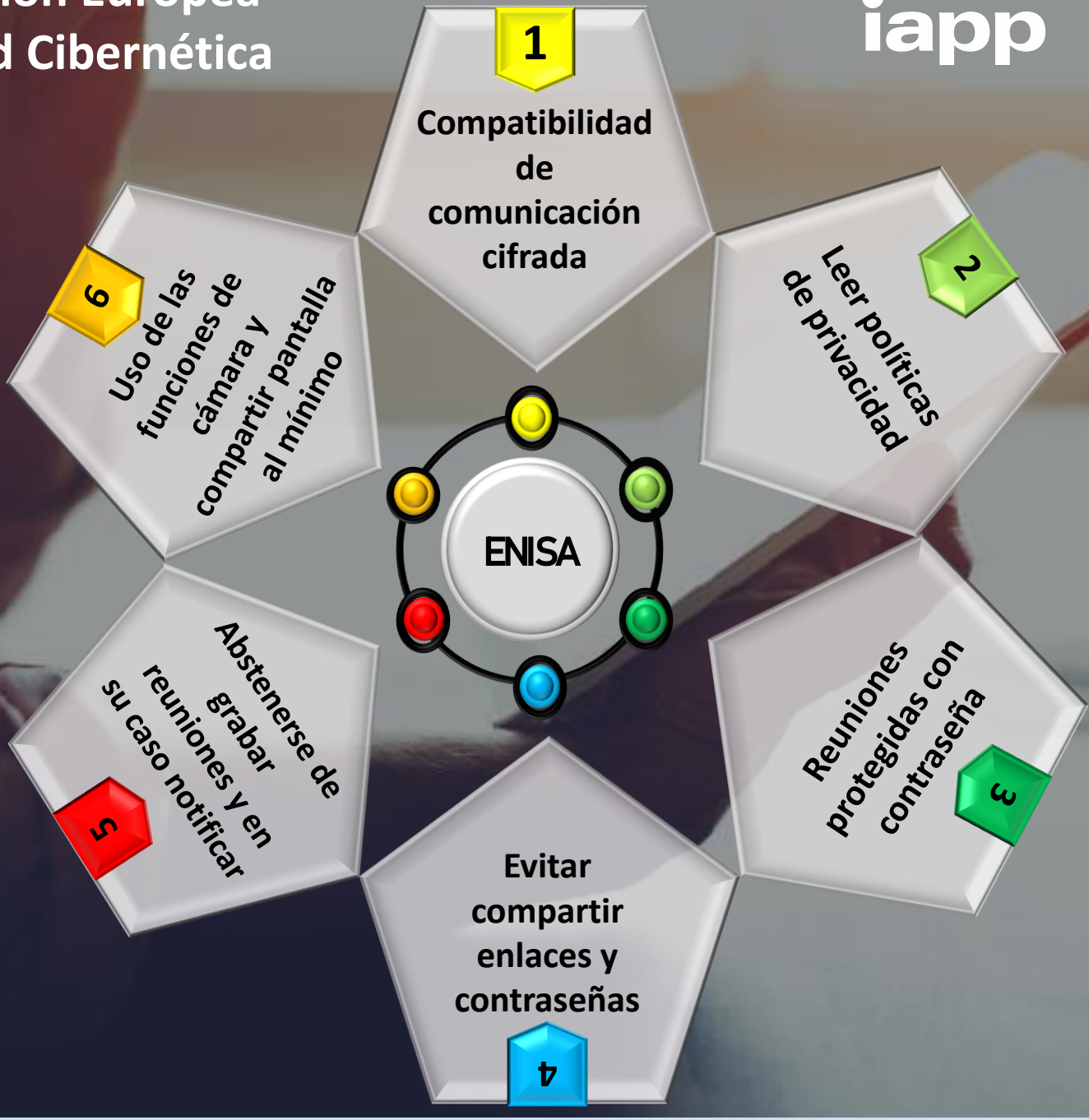
- **Teletrabajo (videollamadas)**
- **Toma de temperatura**
- **Telemedicina**

Teletrabajo

Las preocupaciones en materia de privacidad y protección de datos personales a que nos enfrentamos durante y después de la crisis, no sólo atañen al ámbito del uso de tecnologías para el seguimiento o rastreo de contagiados y sus contactos. Las medidas de distanciamiento social, ha disparado el uso de herramientas de comunicación en línea como conferencias de video, audio, mensajería instantánea, transmisión de documentos o archivos por Internet, que son clave para seguir nuevos regímenes de trabajo y escolares.

Agencia de la Unión Europea para la Seguridad Cibernética (ENISA)

Consejos:



En cuanto a la protección de datos personales e información durante reuniones virtuales el INAI ha detectado algunos de los principales riesgos a los que nos enfrentamos y que los responsables deberían garantizar para evitar cualquier tipo de vulneración:

1. Accesos no autorizados a la sesión virtual.

2. Exposición información confidencial o datos personales a personas no autorizadas

3. software malicioso que utilizan el nombre del programa o aplicación que realiza la reunión virtual

4. Recopilación no autorizada de información de perfiles de redes sociales del usuario, en el caso de que para el inicio de sesión se utilicen este tipo de cuentas.

De igual manera, el INAI ha emitido algunas de las recomendaciones para proteger los datos personales en reuniones virtuales, tales como:

- Leer con atención las políticas de privacidad
- Descargar el software para la reunión de sitios oficiales
- Revisar los permisos solicitados por el software para ejecutarse en los equipos de cómputo
- Evitar asociar cuentas de correo electrónico a redes sociales

PROTECCIÓN DE DATOS PERSONALES durante el trabajo a distancia

inai iapp

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.

PROTECCIÓN DE DATOS PERSONALES durante el trabajo a distancia

inai

iapp

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).

PROTECCIÓN DE DATOS PERSONALES durante el trabajo a distancia

inai

iapp

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.

Toma de temperatura

Las empresas poseen la responsabilidad exigible de proteger a los colaboradores sin escatimar ningún esfuerzo o inversión. Pero al mismo tiempo, deben concientizar a sus colaboradores y personal que opere en los centros de trabajo a la reciprocidad en este cuidado, debiendo tomar las medidas necesarias para evitar cualquier tipo de riesgo a su salud, la de su grupo de trabajo y consecuentemente, a la operatividad de la compañía.

Los puntos clave de la Guía son:

El simple hecho de leer la temperatura de un individuo con un termómetro básico (manual) no constituye el procesamiento de datos personales de acuerdo con el RGPD.

En la medida en que los controles de temperatura involucren el procesamiento de datos de salud, debe cumplirse uno de los fundamentos legales previstos en el Artículo 9 del RGPD.

Si bien los empleadores tienen la obligación de garantizar la salud y la seguridad en el lugar de trabajo, esta obligación no es lo suficientemente específica como para legitimar el procesamiento de datos de salud con fines de monitoreo de COVID-19. Por lo tanto, sugiere legislar para llenar este vacío legislativo en la medida necesaria en el contexto actual.

El DPA belga finalmente enfatiza que los controles de temperatura son solo parcialmente efectivos para detectar COVID-19, ya que no todos los pacientes infectados tienen fiebre, y la fiebre podría ser un síntoma de una enfermedad diferente.

iapp

PRIVACY & INFORMATION SECURITY LAW BLOG

Global Privacy and Cybersecurity Law Updates and Analysis

Home » Belgian DPA Publishes Guidance On Temperature Checks For COVID-19 Monitoring

Belgian DPA Publishes Guidance on Temperature Checks for COVID-19 Monitoring

Posted on June 9, 2020

El 5 de junio de 2020, la Autoridad belga de Protección de Datos publicó una guía sobre los controles de temperatura durante la crisis COVID-19. La Guía tiene como objetivo proporcionar asesoramiento a las organizaciones que buscan controlar el acceso a sus instalaciones restringiendo a las personas con fiebre para evitar una mayor propagación del virus.

Experiencias internacionales

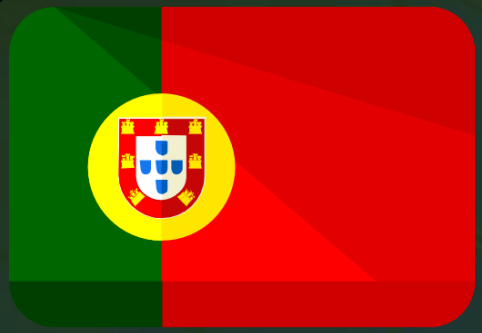
Agencia Española de Protección de Datos:

La temperatura es un dato personal cuyo uso indebido puede implicar una injerencia negativa en la vida privada de los individuos, puede generar discriminación.

En el ámbito laboral, podría tener legitimidad solo si es parte del protocolo emitido por las autoridades sanitarias.

El consentimiento no puede ser la base jurídica, no se puede negar el acceso a una persona a un espacio público por tener una temperatura superior a la media, ya que no necesariamente significa que esté contagiado.

Experiencias internacionales



Comisión Nacional de Protección de Datos de Portugal

En el contexto laboral, el empleador no tiene legitimidad para tomar la temperatura de los empleados, salvo que lo realice personal de salud o el propio trabajador, en tanto que no existe fundamento legal en ningún caso, el consentimiento no es libre y podría condicionar el acceso a cualquier espacio, además de no ser una medida que favorezca de manera eficaz la contención del virus.

Consejo para la Transparencia de Chile

El uso de dispositivos de control de temperatura implica una injerencia en la vida privada de los titulares, pues es un dato sensible que permite determinar que una persona tiene una enfermedad. Además, puede ocasionar que se le niegue a una persona el acceso a un espacio público, violando sus derechos.

CASOS DE COVID-19

INAI EMITE RECOMENDACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES Y EVITAR DAÑO O DISCRIMINACIÓN DE LA PERSONA AFECTADA

Responsables del sector privado y público

- Las organizaciones e instituciones deben proteger la confidencialidad sobre cualquier dato personal o sensible relacionado con algún caso de COVID-19.
- Toda comunicación que se realice en la organización o institución sobre la posible presencia de COVID-19 en el lugar de trabajo, no debe identificar a ningún colaborador de forma individual.
- El tratamiento de datos personales ante el COVID-19, debe ser informado y el titular debe conocer en todo momento las finalidades para las cuáles serán recabados y tratados sus datos personales. Previo al tratamiento, el responsable deberá poner a disposición del titular el aviso de privacidad correspondiente.
- La identidad de las personas afectadas de COVID-19 no debe divulgarse, en caso de requerirse una transferencia de datos personales a las autoridades de salud, ésta deberá ser documentada claramente, fundamentada y realizarse considerando medidas de seguridad que garanticen la protección de los datos personales.
- Los responsables deben definir o seguir los plazos de conservación establecidos en la normativa aplicable, para el tratamiento de los datos personales relacionados con casos de COVID-19, así como los mecanismos que se emplearán para eliminarlos de forma segura, tomando en consideración la normatividad sectorial en la materia.

inai

Telinai 800 8354324

Telemedicina

Las preocupaciones en materia de privacidad y protección de datos personales a que nos enfrentamos durante y después de la crisis sanitaria que vivimos, no sólo atañen al ámbito del uso de tecnologías para la educación a distancia, el teletrabajo o el rastreo contactos. Las medidas de distanciamiento social han provocado la búsqueda de atención de usuarios de diversos servicios, entre ellos el de la salud, por lo que el uso de la telemedicina ha ido aumentado convirtiéndola en una alternativa primordial para dar asistencia médica.

De esta manera, el servicio médico sea trasladado a consultas en línea y el intercambio de mensajería para dar seguimiento y atención a los pacientes mediante correos electrónicos o mensajería instantánea. Por ende, esta práctica conlleva la transmisión de datos personales, en especial, de datos sensibles, motivo por el cual dicha transmisión y posterior almacenaje debe realizarse mediante las herramientas o plataformas adecuadas que garanticen la seguridad de la información personal de los pacientes, cumpliendo de manera estricta los principios y deberes que exige la legislación en esta materia.

Experiencias internacionales

Autoridad Nacional de Protección de Datos Personales de Perú

Cuentan con una norma específica que busca fomentar la eficacia de la Telemedicina, al tiempo que garantiza el debido uso de los datos personales.

Unidad Reguladora y de Control de Datos Personales de Uruguay

Cuentan una ley sobre telemedicina (todos los datos son de carácter sensible). Los responsables deben garantizar medidas adicionales en el tratamiento de los datos.

CASOS DE COVID-19

INAI EMITE RECOMENDACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES

- El tratamiento de datos personales que incluyen datos de salud, deben ser proporcionales bajo la orientación o instrucción de la Secretaría de Salud o autoridades competentes.
- Las instituciones y prestadoras de servicios de salud públicos y privados deben recabar solamente los datos personales mínimos necesarios, para prevenir o contener la programación.
- Los datos personales recopilados con el fin de prevenir o contener la propagación, no deben utilizarse para propósitos distintos.
- Proteger la confidencialidad sobre cualquier dato personal sensible para evitar daño o discriminación de la persona afectada.
- Evitar proporcionar información que permitan identificar a cualquier colaborador afectado por COVID-19.
- El titular debe conocer en todo momento las finalidades para las cuales serán recabados y tratados los datos personales.
- La identidad de las personas no debe divulgarse, en caso de transferencia de datos personales deberá estar debidamente documentada y fundamentada, garantizando las medidas de seguridad.
- Los responsables deben definir o seguir los plazos de conservación de los datos personales, así como los mecanismos de eliminación de forma segura.

EL INAI TE RECUERDA

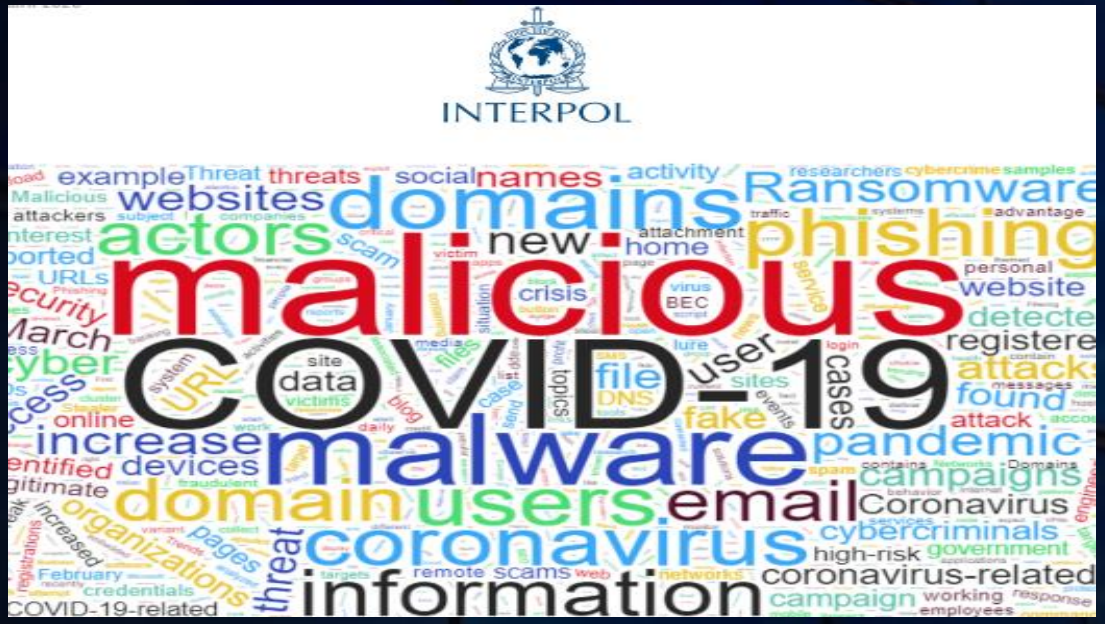
Existe el derecho a la protección de datos personales, por lo que, en caso de un tratamiento inadecuado el INAI te defiende.

inai

Telinai 800 8354324

Otras amenazas

Un gran número de delincuentes oportunistas se están aprovechando de la pandemia de COVID-19 para lanzar diversos tipos de ciberataques. En particular, desde el inicio del brote se han vuelto a detectar varios malware que se encontraban en estado relativamente latente y que han adoptado nuevas formas o cuyos autores han utilizado la COVID-19 para dar un nuevo impulso a sus tácticas de ingeniería social.



PANORAMA MUNDIAL DE LA CIBERAMENAZA RELACIONADA CON LA COVID-19

#WashYourCyberHands

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

¡NO PONGAS EN RIESGO TUS DATOS PERSONALES!

iapp

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.

FRAUDES MÁS UTILIZADOS

EN LA EMERGENCIA SANITARIA POR COVID-19

#TusDatosValen
#INAITeDefiende

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

iapp

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.


DATOS PERSONALES
SEGUROS
COVID 19
inai
OBJETIVO
MINUTO A MINUTO
COVID-19 Y LA PROTECCIÓN DE DATOS PERSONALES
DERECHO DE LOS TITULARES A LA PROTECCIÓN DE SUS DATOS PERSONALES
REPORTAR UN TRATAMIENTO INDEBIDO DE DATOS PERSONALES
RECOMENDACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES ANTE COVID-19
RECOMENDACIONES AUTORIDADES DE PROTECCIÓN DE DATOS PERSONALES
PREGUNTAS FRECUENTES SOBRE TRATAMIENTOS DE DATOS PERSONALES ANTE COVID-19
INFOGRAFÍAS
DOCUMENTOS DE INTERÉS
REPORTAR UN TRATAMIENTO INDEBIDO DE DATOS PERSONALES
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.

Reflexiones al futuro

Adaptarnos al “nuevo normal”, representará estar atentos a las constantes amenazas que el futuro tecnológico nos depare, así como a las soluciones al corto plazo al terminar esta crisis que nos harán replantearnos algunas de las siguientes cuestiones:

- Trabajo a distancia y plataformas virtuales.
- Servicio a domicilio y perfilado de consumo.
- Comercio digital y ciberseguridad.
- Aplicaciones de geolocalización y rastreo de contactos.
- Convergencia de normatividad de datos personales en situaciones globales de emergencia.

¡Gracias!

Mtro. Jonathan Mendoza Iserte
Secretario de Protección de Datos Personales

JonnhyMendoza