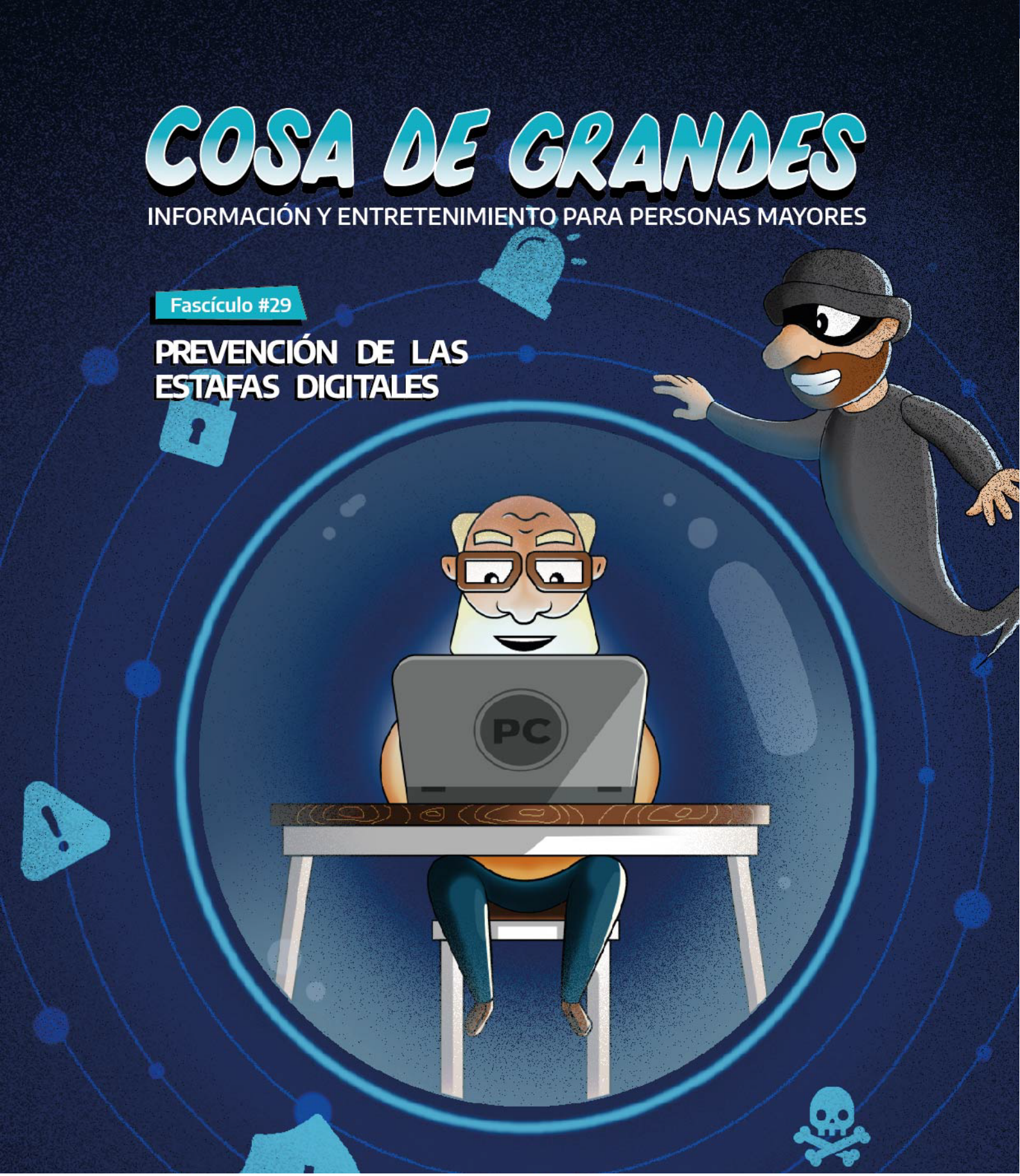
COSA DE GRANDES

INFORMACIÓN Y ENTRETENIMIENTO PARA PERSONAS MAYORES

Fascículo #29

PREVENCIÓN DE LAS ESTAFAS DIGITALES



GOBIERNO DE LA PROVINCIA DE
BUENOS AIRES

¡Hola!

La acelerada incorporación de las Tecnologías de la Información y la Comunicación (TIC) en la vida cotidiana nos ha dado la posibilidad de realizar trámites y otras acciones a través de nuestro celular o computadora, como si el personal del banco, la médica o el comerciante estuvieran disponibles para nosotros, en el lugar y hora que lo necesitemos.

Pero estas ventajas también tienen una contracara. En paralelo al incremento en el uso de las TIC, distintas formas de delitos se fueron adaptando a los entornos digitales. Convencidos de que **tener información confiable y estar prevenidos logra evitar estos abusos o estafas**, es que compartimos estas páginas de *Cosa de Grandes*, que pueden servirnos para estar protegidos y para ayudar a prevenir a otras personas de nuestra familia y comunidad.

Nadie está exento de caer en estos engaños o delitos, por eso, **el Estado provincial, implementó el Programa Interministerial "Cuidarnos en Red"** para dar respuestas frente estas situaciones y también prevenirlas.

¡Ayudanos a compartir este material con otras personas!

ÍNDICE

Quienes quieran leer y compartir los fascículos ya publicados de la serie *Cosa de Grandes*, pueden hacer **clic aquí**.

Estos materiales son producidos por el Ministerio de Comunicación Pública de la Provincia de Buenos Aires.

Para comunicarse con nosotros, pueden escribir a:
cosadegrandes@gba.gob.ar

Las tecnologías en nuestra vida

A lo largo del tiempo, **hemos incorporado el uso de distintas tecnologías que llegaron para facilitarnos la vida cotidiana**. Así sucedió hace algunos años con la aparición del televisor, del lavarropas o el télefono fijo y, en la actualidad, con las Tecnologías de la Información y la Comunicación (TIC) que ocupan cada vez más lugar en nuestro día a día.

Quienes nos animamos a navegar por internet descubrimos un sinfín de posibilidades, por ejemplo, hacer trámites y acceder a servicios sin movernos de casa. Con la pandemia, esos recursos se han multiplicado. Pero **es importante que durante estas actividades tomemos ciertas precauciones**, así como lo hacemos en otros ámbitos de la vida.

Los diferentes modos de uso de las TIC no escapan a otras realidades y **podemos encontrarnos con situaciones no deseadas, como los ciberdelitos o estafas digitales**. Así como tenemos la costumbre de estar atentos a distintos cuidados, como cerrar la puerta con llave, evitar hablar con extraños o resguardar nuestras pertenencias en el transporte público, **tenemos que estar prevenidos cuando realizamos acciones a través de internet, para estar más seguros y protegidos**.

Ciberdelitos

Ciberdelitos: son estafas que se producen a través de internet, aunque en algunas de sus etapas pueden utilizar otros recursos, como el teléfono. Los estafadores son denominados ciberdelincuentes y cometen distintos actos ilegales, como robo de datos personales o de identidad para manipular nuestras cuentas bancarias, realizar ataques discriminatorios y acoso, entre otras modalidades.

La ciberdelincuencia es una problemática que nos afecta a todos: niños, niñas y adolescentes, adultos y personas mayores. Por eso, **tenemos que estar prevenidos para cuidarnos**.

Quienes cometen los ciberdelitos lo hacen de manera premeditada y siguiendo algunos patrones. A continuación, ponemos en común los más frecuentes:

- **Ponen en práctica el famoso "cuento del tío"**: nos dicen que ganamos un premio o que el banco está solicitando que retiremos el dinero de nuestra cuenta, entre otras excusas. **Puede ser que nos contacten por teléfono, redes sociales, correo electrónico o mensajes de texto**.

- **Se presentan como integrantes de un banco o de una entidad oficial**, como la ANSES o cualquier otra, y en la charla comentan alguno de nuestros datos como si nos conocieran. **Buscan ganar nuestra confianza** haciéndose pasar por un organismo público o empresa.

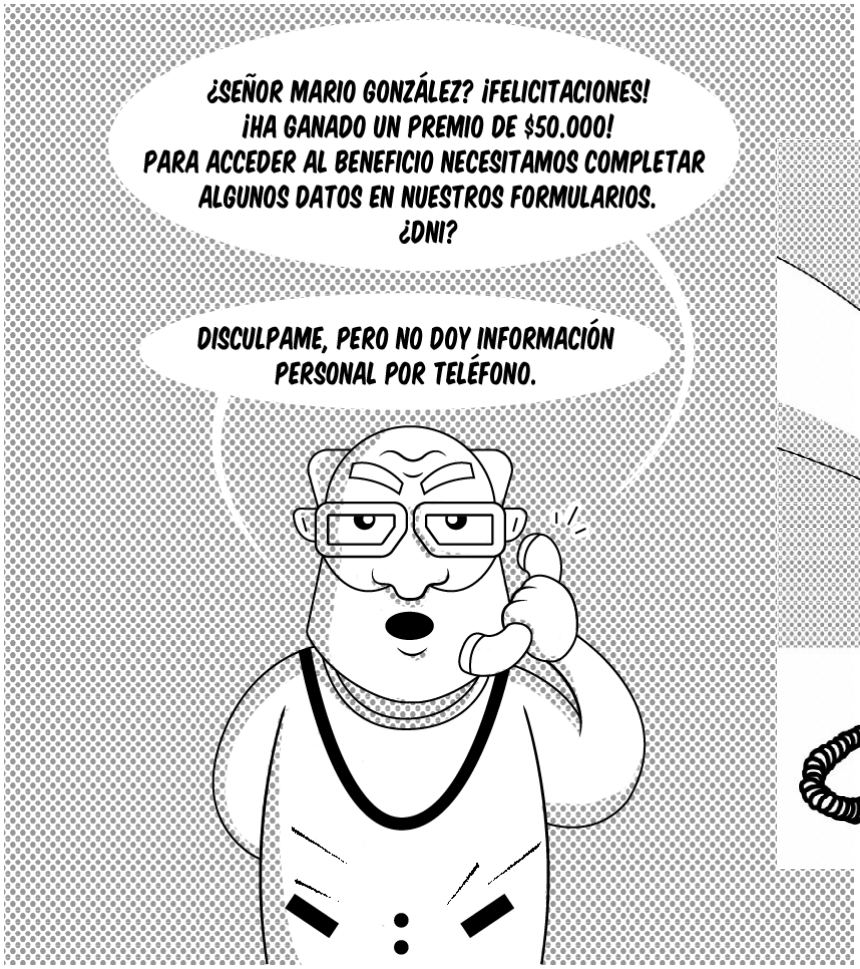
Generan una conversación para que brindemos datos confidenciales o que realicemos transacciones bancarias. Su estrategia es expresar una supuesta urgencia para descolocarnos, engañarnos y obtener nuestros datos personales.

Nos envían *links* a través de *WhatsApp*, correo electrónico o mensaje de texto para descargar algún programa o ingresar a un sitio *web*, **con la intención de robarnos contraseñas o afectar el buen funcionamiento de la computadora, *tablet* o celular**. ¿Cómo detectar si el *link* es seguro? Cuando posamos el mouse en el enlace (sin cliquear) y aparece una vista previa de la página, es confiable; de lo contrario, es probable que sea un virus.

Usan los datos personales de manera fraudulenta: realizan compras, solicitan préstamos o vacían nuestras cuentas.

Ningún banco, institución o empresa nos va a solicitar datos personales o de nuestras cuentas. Las acciones bancarias se realizan a través de las *apps*, páginas *web* oficiales o de manera presencial.


HOLA TE LLAMO DE PARTE DE TU NIETO.
¿QUIÉN, MARTÍN?


¿SEÑOR MARIO GONZÁLEZ? ¡FELICITACIONES!
¡HA GANADO UN PREMIO DE $50.000!
PARA ACCEDER AL BENEFICIO NECESITAMOS COMPLETAR ALGUNOS DATOS EN NUESTROS FORMULARIOS.
¿DNI?
DISCULPAME, PERO NO DOY INFORMACIÓN PERSONAL POR TELÉFONO.


PAF!

Diez recomendaciones para navegar seguros

Ahora que ya conocemos algunos patrones sobre cómo operan los ciberdelincuentes, podemos estar más atentos y prevenidos frente a las estafas en entornos digitales. Aquí les compartimos algunos consejos para **adoptar buenas prácticas** y así **fortalecer nuestra seguridad *online***.

Con quiénes nos comunicamos

1. Siempre leamos con atención quién es el remitente de los mensajes que nos llegan a través del correo electrónico o del celular. **Nunca abramos enlaces de desconocidos. ¡Esos *links* pueden ser virus!**

2. Asegurémonos de que las **cuentas** de las entidades con las que nos comunicamos por redes sociales sean **oficiales**. Una cuenta con la insignia azul y el tic blanco garantiza que existe una verificación de autenticidad.

Las contraseñas

3. Repetir la misma contraseña en distintas cuentas las hace más vulnerables.

4. Evitemos que tengan relación directa con nuestros datos personales básicos.

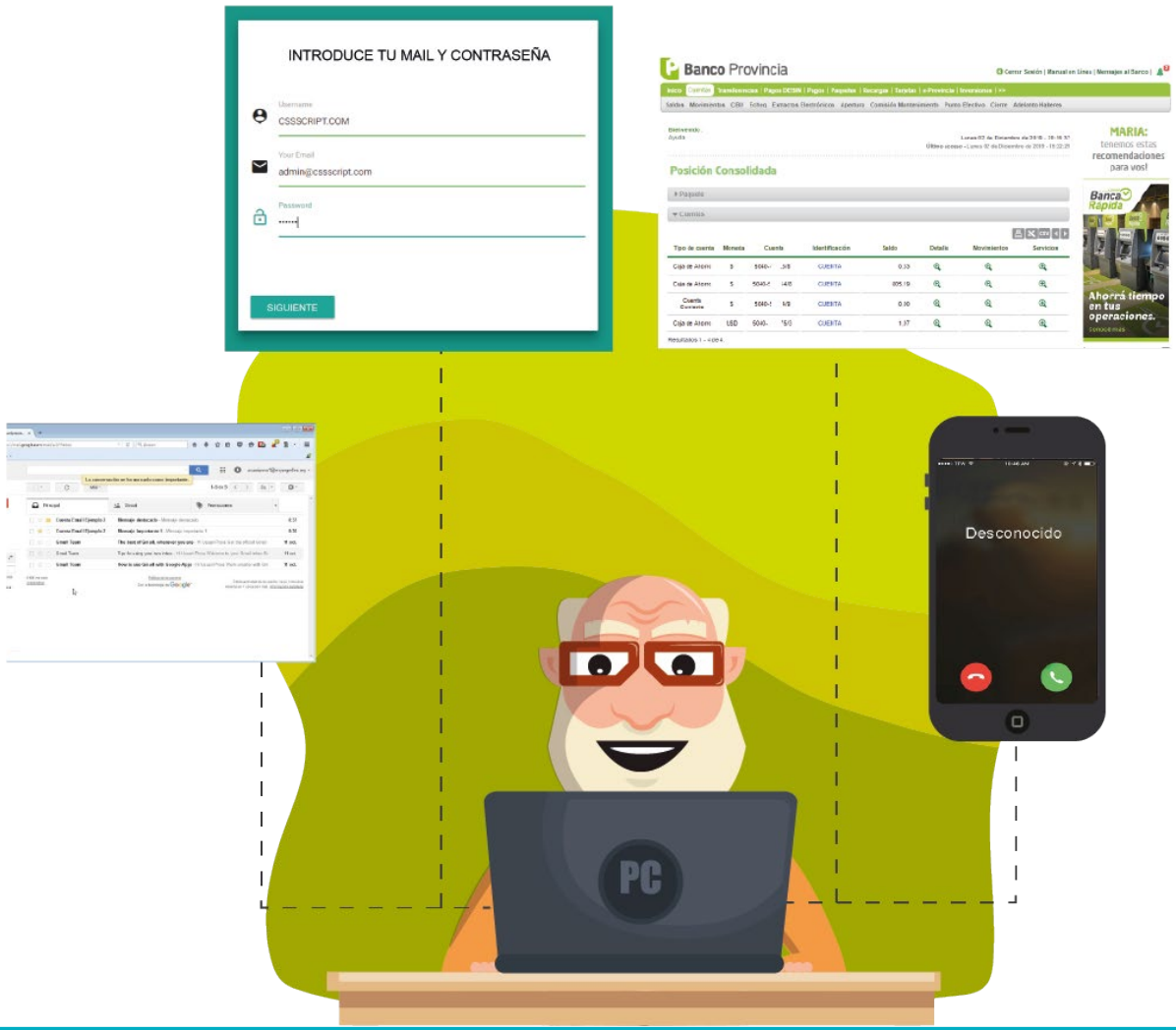
5 Para que sean más seguras, sirve mezclar mayúsculas con minúsculas, números y/o caracteres especiales (-, _, /, #, !).

6 **Nunca compartamos con otras personas nuestros nombres de usuario y contraseñas.**

Las compras *online*

7 Desconfiemos de las ofertas o promociones demasiado atractivas: podríamos estar ante una situación fraudulenta.

8 Asegurémonos de que en el sitio *web* aparezca identificado el responsable del comercio y su ubicación.



Las cuentas bancarias

9 **Verifiquemos periódicamente los movimientos de nuestras cuentas**, así sabremos exactamente qué sucede con ellas.

10 Si nos contactan por llamada, *WhatsApp*, correo electrónico o mensajes de texto para confirmar o solicitar información, **cortemos la comunicación**, por más que se presenten como representantes de bancos o instituciones. **Los entes oficiales nunca nos solicitarán claves y/o contraseñas**.

Banco Provincia

En el canal oficial de *YouTube* del Banco de la Provincia de Buenos Aires encontraremos una serie de videos sobre los modos de uso de sus aplicaciones con algunas recomendaciones. Específicamente, es conveniente que veamos **"Consejos de seguridad" para saber cómo operar sin ir al banco y de un modo seguro**. Podemos acceder haciendo clic **aquí**.

Quienes realizan estafas digitales usan el factor sorpresa a su favor e intentan apurarnos usando excusas. **Tener información sobre cómo actúan y tomarnos nuestro tiempo sin entrar en su juego es el mejor modo de prevenirnos**.

Glosario

Existen muchas formas de delitos en entornos digitales. Conozcamos algunas de estas modalidades:

- ***Phishing, vishing* y *smishing***: son formas de estafa *online* en las que los defraudadores simulan ser de sitios oficiales para "pescar" (*to fish/fishing*, en inglés) información personal y financiera engañando a las víctimas inadvertidas. ¿Cuáles son sus diferencias? El *phishing* se refiere al envío de mensajes masivos a través de correos electrónicos o sitios *web* ficticios. El *vishing* tiene el mismo propósito, pero la modalidad es a través de llamadas telefónicas. Y el *smishing* nombra la forma de estafa que se realiza a través de mensajes de texto o *WhatsApp*.

- ***Grooming***: refiere al contacto a través de internet de una persona adulta con una niña, niño o adolescente con el propósito de cometer un delito contra su integridad sexual, obligándolos –mediante la manipulación y el engaño– a enviar imágenes o a generar un encuentro presencial.

- **Sextorsión**: consiste en una forma de chantaje en la que se amenaza a la víctima con la divulgación de imágenes íntimas a cambio de dinero o para presionar la realización de alguna otra acción bajo este condicionamiento.

Frente a este tipo de actos ilegales, es fundamental generar la denuncia en cualquiera de los organismos que trabajan en el **Programa interministerial "Cuidarnos en Red"**.

Entrevista a Lisandro Pellegrini

“Cuidarnos en Red”

Lisandro Pellegrini nació en Bernal, partido de Quilmes. Es abogado especialista en derecho penal. En la actualidad, es el titular de la Subsecretaría de Política Criminal del Ministerio de Justicia y Derechos Humanos de la Provincia de Buenos Aires y, basado en su labor diaria, sostiene: **“tratamos de que todos los recursos del Estado provincial vinculados a la persecución penal, se organicen de la manera más eficiente y estratégica posible”**.

El 13 de abril de 2021, **el Gobierno provincial presentó “Cuidarnos en Red”, un Programa interministerial destinado a la prevención de delitos en entornos virtuales**.

“Cuidarnos en Red” está integrado por los siguientes ministerios: Justicia y Derechos Humanos; Mujeres, Políticas de Género y Diversidad Sexual; Desarrollo de la Comunidad; Producción, Ciencia e Innovación Tecnológica, y la Subsecretaría de Salud Mental, Consumos Problemáticos y Violencias en el ámbito de la Salud. Además, colaboran el Instituto de Políticas Públicas de Prevención del Grooming de la Cámara de Diputados y la Defensoría del Pueblo de la Provincia.

Lisandro Pellegrini, subsecretario de Política Criminal de la Provincia de Buenos Aires.

Una política integral contra los delitos digitales

Lisandro cuenta que "Cuidarnos en Red" se gesta a partir de reconocer que los conflictos en entornos digitales crecieron exponencialmente desde que comenzó la pandemia por COVID-19: **"En abril de 2020 identificamos que la ocurrencia de delitos y de otras conflictividades en entornos digitales se disparaba, y no solo en la Argentina, sino en el mundo"**, y detalla: "en la provincia los indicadores dan cuenta de que el *grooming* y los abusos infantiles en entornos digitales aumentaron en un 80%".

En el programa se visibilizan tres manifestaciones concretas de la ciberdelincuencia: el ***grooming***, que es el acoso sexual a niños, niñas y adolescentes por parte de personas adultas en entornos digitales; **la violencia de género en entornos digitales**, relacionada con la exposición y difusión sin consentimiento de imágenes íntimas de mujeres o personas del colectivo LGTB+ y asociada a formas extorsivas, y **las ciberestafas**.

Respecto de esta última modalidad, el Subsecretario de Política Criminal explica que "**el comportamiento de un estafador se dirige a manipular a otra persona, engañarla y, a través de esa conducta, sacarle algún dato**, una clave, un usuario, un número de tarjeta, para **generarle un perjuicio económico**, por ejemplo".

Si bien los registros indican que cualquier persona bancarizada es una víctima potencial de estafas en entornos digitales, desde "Cuidarnos en Red" identifican que las personas mayores son uno de los principales grupos poblacionales que se ve afectado por estos delitos.

Prevenir y sensibilizar

Lisandro destaca que “el programa está orientado a prevenir y sensibilizar en este tema” pero que además contiene una parte penal, en cuyos casos el Ministerio de Justicia y Derechos Humanos se ocupa de hacer un seguimiento del proceso para que llegue a un buen resultado.

El espíritu del Programa es prevenir los delitos en entornos digitales. Hacerlos visibles y conocer cómo vienen operando las ciberestafas es una forma de que estos actos ilegales pierdan eficacia ante una sociedad más atenta.

“Cuidarnos en Red” se caracteriza por la articulación entre múltiples actores del Estado que trabajaron en generar acuerdos para identificar cada ciberdelito y determinar de qué manera se abordaría. Así, se lograron construir las Guías de actuación. Actualmente se trabaja en la formación de los trabajadores que se encuentran directamente con las personas afectadas, y en la construcción de redes institucionales con los 135 municipios de la provincia de Buenos Aires para una implementación articulada.

Podemos acceder a las Guías de Actuación haciendo clic aquí.

Cómo, dónde y para qué denunciar

Desde “Cuidarnos en Red” resaltan que **ningún operador del Estado ni de un banco puede llamar para pedirnos una contraseña o un número de tarjeta**. En caso de haber atendido un llamado de este tipo y haber informado alguno de estos datos, el entrevistado sugiere que: “**primero hay que llamar al banco para que congele todo el daño que se pueda producir** a partir de la información aportada al ciberdelincuente y, luego, hacer la denuncia en la policía o en la fiscalía”.

Es conveniente realizar la denuncia lo más rápido posible.

Para los casos de **ciberestafas** se cuenta con la **línea telefónica 148** que es gratuita y tiene una **derivación al área del consumidor** del Ministerio de Producción, Ciencia e Innovación Tecnológica, donde las personas serán orientadas para saber cómo actuar.

En el caso de ***grooming*** podemos comunicarnos con la **línea 102** o acercarnos a los **Centros de Acceso a la Justicia** o a los **Centros de Protección de los Derechos de la Víctima** de nuestra localidad. Ante los casos que tengan que ver con **violencia de género** se puede recibir acompañamiento en la **línea 144**.

Denunciar un delito en entornos digitales es una forma de defender nuestros derechos.

Recomendaciones

#QuedateEnCasa

Estamos llegando a fines de abril con un aumento de casos de COVID-19 significativo, en el contexto de la denominada segunda ola. Sigamos respetando las medidas de prevención y cuidémonos entre todos. #LavateLasManos #VentiláLosAmbientes #UsáTapabocasYNariz #2MetrosDeDistancia

El amor menos pensado es una película argentina que se estrenó el 2 de agosto de 2018. Con las actuaciones de Mercedes Morán, Ricardo Darín y un elenco extenso, esta comedia plantea una encrucijada primordial de nuestra vida moderna: ¿Nos conformamos o somos francos y vamos por más? ¿Cuál es la edad para proyectar lo que queremos de nuestra vida? En un contexto de metrópolis se sucede una historia que nos hace reír y pensar. Podés verla por YouTube haciendo **clic aquí**.

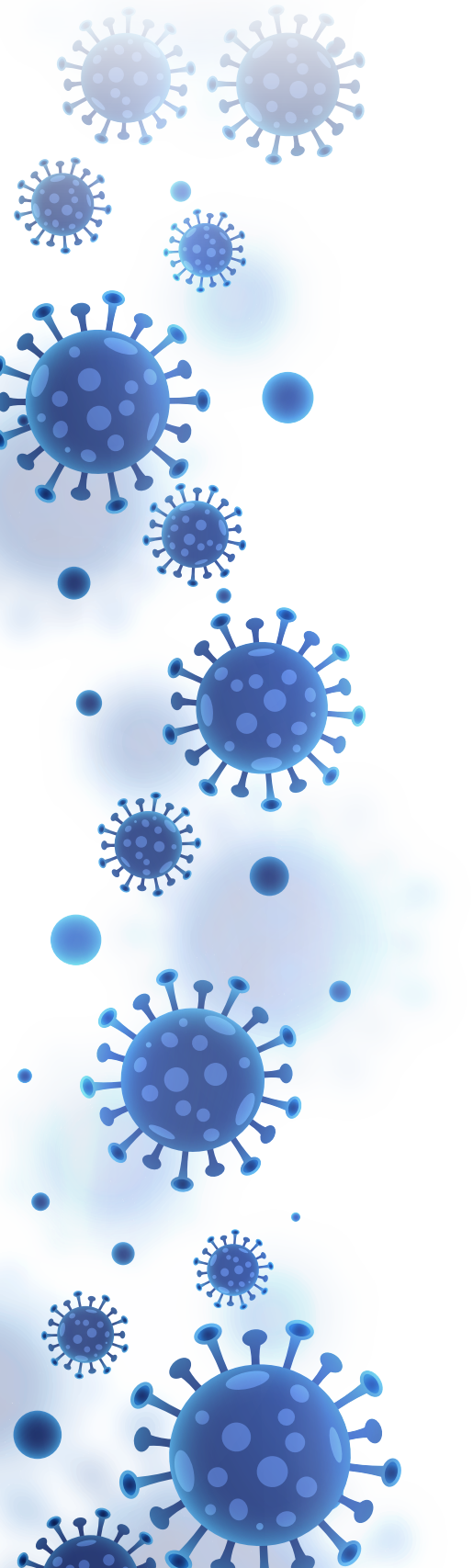
Juan Falú y Liliana Herrero protagonizan este ***homenaje al disco Leguizamón-Castilla***, a 20 años de su grabación. Con una puesta íntima y de entrecasa en el Auditorio Nacional, el concierto recorre varios de los temas del disco original que se entrelazan con la conversación amena de estos grandes músicos populares argentinos. La apuesta y el trabajo del Centro Cultural Kirchner, una vez más, se vuelve inspiradora y emocionante cuando traen los recuerdos, la música y la palabra hasta nuestra casa. Para verlo y escucharlo hacé **clic aquí**.


BUENOS AIRES
VACUNATE
Ya se vacunaron
más de 1.600.000
personas mayores
MÁS CERCA DE LO QUE QUEREMOS VOLVER A DISFRUTAR
REGISTRATE EN
vacunatepba.gba.gob.ar
DESCARGATE LA APP
VACUNATEPBA
Available on the App Store
Google Play
GOBIERNO DE LA PROVINCIA DE
BUENOS AIRES

JUEGOS DE LA PROVINCIA

Para jugar solos o en compañía

¿Qué sabemos sobre el COVID-19?
(Buscá las respuestas al final del material)



1. Los coronavirus son un tipo de virus que solo afectan a los humanos.

¿Verdadero o Falso?

2. El primer caso de COVID-19 en Argentina fue confirmado el 3 de marzo de 2020.

¿Verdadero o Falso?

3. Se llama pandemia a la expansión de una enfermedad en al menos cinco países.

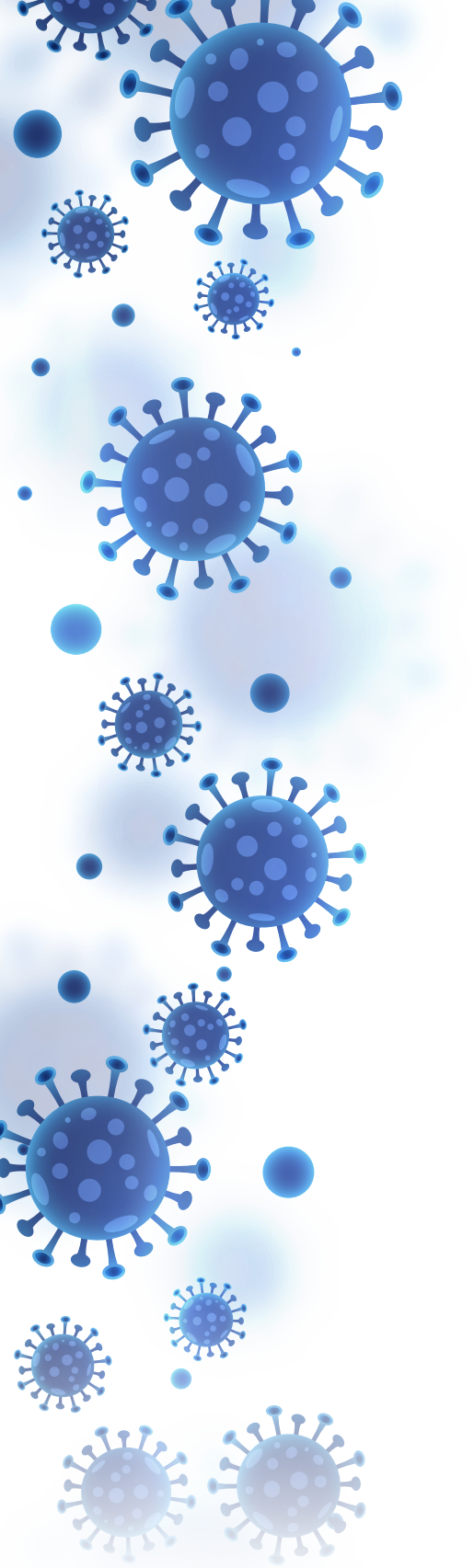
¿Verdadero o Falso?

4. Las científicas y los científicos del CONICET y del Instituto Leloir tardaron 100 días para desarrollar los primeros análisis serológicos que permiten detectar la presencia de anticuerpos contra el COVID-19.

¿Verdadero o Falso?

5. Fue un bonaerense quien descubrió el uso del plasma convaleciente, que hoy se utiliza para la recuperación de pacientes críticos infectados por COVID-19.

¿Verdadero o Falso?



6. Una persona que tuvo COVID-19 y sanó, no puede volver a contagiarse. Entonces, no necesita aplicarse la vacuna.

¿Verdadero o Falso?

7. Se considera “contacto estrecho” a las personas que hayan estado en contacto con otra persona con COVID-19 mientras presentaba síntomas o durante las 48 horas previas al inicio de los mismos.

¿Verdadero o Falso?

8. Para que una vacuna sea aplicada masivamente necesita de la aprobación de revistas científicas internacionales.

¿Verdadero o Falso?

9. La aprobación de una vacuna para su aplicación masiva atraviesa al menos cinco instancias de evaluación y control rigurosos.

¿Verdadero o Falso?

Respuestas correctas

1. FALSO.
Los coronavirus son una familia de virus conocida por causar enfermedades respiratorias. Afectan a **numerosas especies de animales**, y algunos de estos virus –incluidos el SARS-CoV-2 o COVID-19, el SARS-CoV, MERS-CoV– pueden afectar a las personas.

2. VERDADERO.
El 2 de marzo de 2020 un establecimiento de salud privado de la Ciudad de Buenos Aires notificó el caso y el Instituto Malbrán realizó los análisis correspondientes. El 3 de marzo fue confirmado por el Ministerio de Salud de la Nación. El paciente era un hombre de 43 años que llegaba de sus vacaciones en Italia.

3. FALSO.
La Organización Mundial de la Salud (OMS) considera como pandemia a la propagación de un virus a **nivel global** donde la mayoría de las personas no tiene inmunidad contra ese virus. El 11 de marzo de 2020, la OMS declaró al COVID-19 como pandemia, en un marco de preocupación por la acelerada expansión del virus que ya registraba casos en 114 países.

4. FALSO.
El análisis serológico fue desarrollado en **tiempo récord: en 45 días** crearon un test que detecta en sangre y suero anticuerpos que el sistema inmune produce para combatir el COVID-19. Si el resultado es positivo, la persona testeada cursó o está cursando la infección.

5. VERDADERO.
La terapia con plasma convaleciente fue desarrollada en la década del 70 por el Dr. Julio Maiztegui, nacido en Bahía Blanca. El uso del plasma permite la transfusión de anticuerpos. Los tratamientos realizados hasta el momento han demostrado disminuir la mortalidad y la cantidad de días de internación de los pacientes con COVID-19. **Si tuviste coronavirus #DonáPlasma**.

6. FALSO.
Cada vez hay mayores evidencias sobre casos de **recontagios de COVID-19**. Por este motivo, es fundamental que, aún después de haber padecido la enfermedad o de haber recibido la vacuna, no se abandonen las medidas de prevención: uso del barbijo, distancia de dos metros, ventilación constante de los ambientes e higiene de manos. Esto nos permite protegernos y proteger a los demás.

7. VERDADERO.
La definición de contacto estrecho es de utilidad para evaluar la necesidad de aislamiento de una persona que ha estado en una situación de riesgo de contagio. En este caso deben realizar un **estricto aislamiento** durante 14 días, aún cuando no presenten síntomas relevantes.

8. FALSO.
Cada país tiene un ente regulador que, en nuestro caso, es la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT). Este organismo ha sido reconocido por la Organización Mundial de la Salud (OMS) y la Organización Panamericana de la Salud (OPS) como Autoridad Regulatoria de Referencia en Medicamentos y Productos Biológicos. Los alimentos y medicamentos que consumimos deben haber sido controlados y aprobados por dicha autoridad.

9. VERDADERO.
La elaboración de una vacuna comienza con una fase exploratoria en la que se produce una fórmula y se aplica en animales. Si supera esa etapa, pasa a Fase I y se prueba la vacuna con un pequeño grupo de personas, con estrictos controles. Si se superan los

estándares de calidad, pasa a Fase II y se amplía el grupo para las pruebas controladas. Luego, en Fase III se completan los análisis de seguridad. Y si supera todas estas instancias, los organismos específicos en cada país, realizan una nueva evaluación general para aprobarla o no. En Argentina, ese organismo es la ANMAT.

GOBIERNO DE LA
PROVINCIA DE
BUENOS
AIRES

gba.gob.ar