ALFABETIZACIÓN Y SEGURIDAD DIGITAL:

LA IMPORTANCIA DE MANTENERSE SEGURO E INFORMADO

OEA | Más derechos para más gente

ÍNDICE

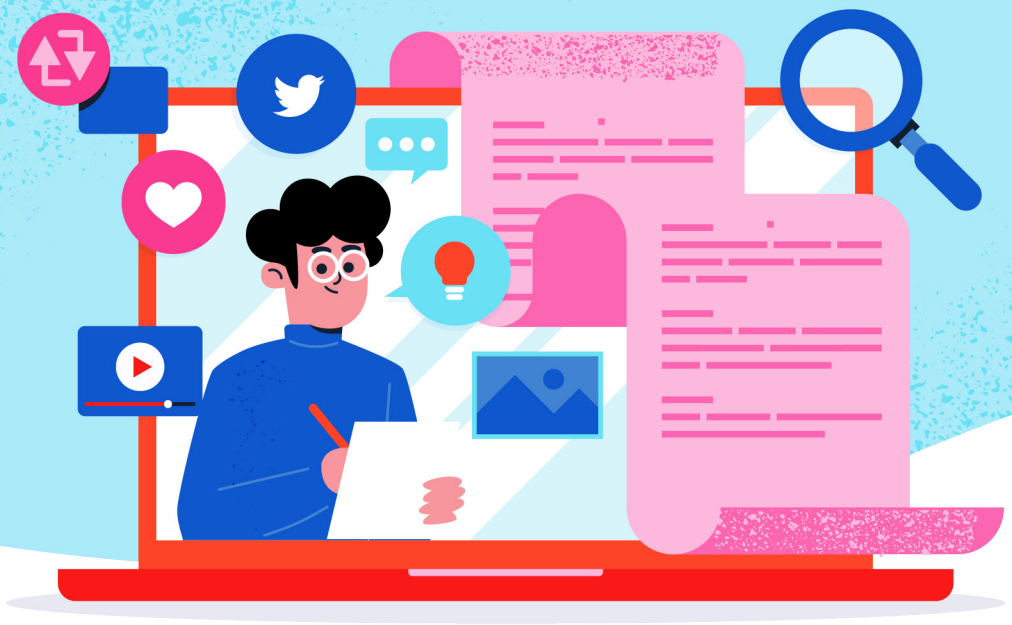
CRÉDITOS

Equipo Técnico Twitter

Andrea Pereira Palacios
Hugo Rodríguez Nicolat

Equipo Técnico OEA

Alison August Treppel
Kerry-Ann Barrett
Gerardo De Icaza
Gonzalo Espáriz
Cristóbal Fernández
Mariana Jaramillo
Yerutí Méndez
Gabriela Montes de Oca
David Moreno
María Isabel-Rivero
Diego Subero
Katya Vera Morales



INTRODUCCIÓN

En la era digital y de redes sociales, la disponibilidad de información inmediata y abundante ayuda a que las personas se mantengan al día de lo que está pasando en el mundo de forma instantánea. Además, la digitalización y la transformación de procesos cotidianos, son dos procesos que ocurren de manera rápida e imparable.

Recibir y procesar la abundante información a la que actualmente se tiene fácil acceso, requiere de ciertas habilidades que se deben desarrollar, así como del entendimiento de los medios en los cuales circula. Es importante conocer no solamente el origen, intención o finalidad de la información que se consume y se publica, sino también los posibles riesgos y el impacto que pueden tener en nuestro entorno.

Ante este escenario, **Twitter** y la **Organización de los Estados Americanos (OEA)** han actualizado esta publicación sobre alfabetización y seguridad digital, con el objetivo de brindar herramientas y presentar buenas prácticas en el monitoreo, consumo y distribución de información, así como recomendaciones para mantenerse seguro en línea, con un particular enfoque en Twitter. En esta edición actualizada de la guía "Alfabetismo y Seguridad Digital: Mejores Prácticas en el uso de Twitter" [1] en septiembre de 2019, se identifican fenómenos adicionales a la edición anterior en materia de desinformación, así como la importancia de la alfabetización en procesos democráticos.

Desde el lanzamiento de la primera edición de esta guía, el mundo ha experimentado un crecimiento vertiginoso en actividades en Internet. De acuerdo con estudios de la Comisión Económica para América Latina y el Caribe (CEPAL) de la Organización de las Naciones Unidas, los avances en la utilización de las redes y la infraestructura de comunicaciones que se preveía que demorarían años en concretarse, se han producido en pocos meses desde el 2020[2]. La CEPAL también señala la necesidad de desarrollar habilidades digitales como un condicionante clave en el aprovechamiento de Internet.

1 Organización de los Estados Americanos y Twitter. (2019). Alfabetismo y Seguridad Digital: Mejores Prácticas en el Uso de Twitter. https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf
2 Comisión Económica para América Latina y el Caribe (CEPAL). Informe Especial COVID-19.(2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19. https://repositorio.cepal.org/bitstream/handle/11362/45938/4/S2000550_es.pdf

Tanto la OEA como Twitter han podido observar diversos cambios en este panorama. En Latinoamérica, más de 30% de empresas percibieron un aumento en el número de ataques cibernéticos en el 2019 en comparación con años anteriores, aunque solo 17% cuenta con un seguro de riesgo cibernético[3]. Esto manifiesta la importancia de proceder en el desarrollo de concientización sobre las amenazas digitales existentes en la región y cómo combatirlas en todos los niveles. Por su parte, Twitter, al ser una plataforma pública y abierta para el intercambio de perspectivas, ideas e información, se mantiene en un proceso constante de actualización de sus reglas, procesos, herramientas y tecnología. Esto es necesario, para la adaptación de la plataforma en paralelo a los cambios que se presentan en la sociedad, y la forma en que las personas interactúan y comparten información en su servicio.

La primera sección de la publicación se centra en definir qué es la alfabetización digital, haciendo referencia al trabajo realizado por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y la Comisión Interamericana de Derechos Humanos (CIDH). Estos enfoques reflejan el desarrollo del término "alfabetización" y su relación con la tecnología, al igual que consideraciones regionales sobre la alfabetización digital. Asimismo, se ha incluido un apartado específico elaborado por la Comisión de Observación Electoral (DECO) de la OEA con respecto a la relación entre la alfabetización digital y la democracia.

La segunda sección está relacionada con buenas prácticas de ciberseguridad, presentando información con respecto a la naturaleza de nuevas amenazas cibernéticas que han surgido desde la primera publicación de esta guía. De igual forma, se incluyen recomendaciones específicas que responden al aumento de las condiciones de teletrabajo o trabajo remoto y al trabajo periodístico en la región.

La tercera sección ha ampliado y actualizado la información referente al consumo de información en Twitter y consejos para verificar su veracidad. También se explican cuáles son algunas de las herramientas disponibles para navegar mejor la plataforma y encontrar y verificar información de una manera fácil y rápida.

Finalmente, en **la última sección** de la guía, dada la importancia de Twitter como herramienta de comunicación, se ofrece una actualización a las Reglas de Twitter y su aplicación, con el propósito de dar a conocer los parámetros que rigen la circulación de información e interacciones en la plataforma. También se explica en esta sección cuáles son las herramientas de seguridad de Twitter y cómo utilizarlas para tener una experiencia más personalizada y controlada en la plataforma.

La tecnología y las herramientas disponibles para su uso están en constante desarrollo, por lo que se insta a todas las personas a mantenerse constantemente atentas a las actualizaciones de productos y políticas que afectan su desenvolvimiento e interacciones en medios digitales y redes sociales.

CONTAR CON HABILIDADES PARA DESENVOLVERSE DE MANERA SEGURA EN EL INTERNET ES FUNDAMENTAL PARA CONTRARRESTAR LOS CIBERATAQUES Y OTROS MECANISMOS DE DESINFORMACIÓN QUE CONTINUAMENTE SON MÁS SOFISTICADOS Y COMPLEJOS.

3 Marsh y Microsoft. (2020). Estado de Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19. https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

ALFABETIZACIÓN DIGITAL

¿Qué es la alfabetización digital?

De acuerdo a la UNESCO, la alfabetización se define como:

> **Un medio de identificación, comprensión, interpretación, creación y comunicación en un mundo cada vez más digitalizado, basado en textos, rico en información y en rápida mutación[4].**

Esta definición, acuñada de forma oficial a partir de años recientes, contempla que las habilidades digitales son un componente fundamental de la alfabetización en general, a diferencia de nociones anteriores que solamente consideran el conjunto de competencias de lectura, escritura y cálculo.

De igual forma, en el anuario de 2016 de la UNESCO, en su sección "Alfabetización de Información Mediática para las Metas para el Desarrollo Sostenible," se encuentran las "Cinco Leyes sobre la Alfabetización de Información Mediática". A saber:

4 Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2016). Alfabetización. https://es.unesco.org/themes/alfabetizacion

1. La información, la comunicación, las bibliotecas, los medios de comunicación, la tecnología, la Internet y otras fuentes de información pertenecen a la misma categoría de tipo de información. Ninguna es más relevante que la otra ni debe ser tratada como tal.
2. Cada ciudadano es un creador de información o conocimiento y tiene un mensaje. Todas las personas deben estar facultadas para acceder a nueva información y expresarse libremente.
3. La información, el conocimiento y los mensajes no siempre están exentos de valores o prejuicios. Cualquier conceptualización, uso y aplicación de alfabetización digital debe presentar este hecho de manera transparente y comprensible para todos los ciudadanos.
4. Todo ciudadano desea conocer y comprender información, conocimientos y mensajes nuevos, así como comunicarse, y sus derechos nunca deben ser comprometidos.
5. La alfabetización digital es un proceso dinámico de experiencias vividas. Se considera completa cuando incluye conocimientos, habilidades y actitudes, cuando abarca el acceso, la evaluación, el uso, la producción y la comunicación de información, de contenido mediático y tecnológico.

Es importante tomar en cuenta estas nociones para así comprender la importancia que tiene la adquisición de herramientas digitales para el correcto uso de Internet por parte de cualquier persona.

¿Cómo lograr la alfabetización digital?

Adquirir herramientas digitales tiene un impacto directo en nuestro nivel de alfabetización. En el anuario de la UNESCO, señalado en el primer apartado de esta sección, se exponen 10 habilidades que deben desarrollarse para lograr la alfabetización digital[5]. Estas habilidades son:

1. Interactuar con información referente a los medios y la tecnología.
2. Ser capaz de aplicar habilidades técnicas de comunicación de información para procesar información y producir contenido mediático.
3. Utilizar, de manera ética y responsable, la información y comunicar su comprensión o conocimiento adquirido a una audiencia o lectores en una forma y medio apropiados.
4. Extraer y organizar información y contenidos.
5. Evaluar de forma crítica la información y el contenido presentado en los medios informativos y otras fuentes de información, incluyendo medios en línea, en términos de autoridad, credibilidad, propósito y posibles riesgos.

5 Grizzle, A and Singh, J. (2016). In the MILID Yearbook 2016: Media and Information Literacy for the Sustainable Development Goals.

6. Localizar y acceder a información relevante.
7. Sintetizar las ideas extraídas del contenido.
8. Comprender las condiciones bajo las cuales se pueden cumplir esas ideas o funciones.
9. Comprender el papel y las funciones de los medios de comunicación, incluyendo medios en línea, en la sociedad y su desarrollo.
10. Reconocer y articular la necesidad de información y de los medios.

La alfabetización digital para combatir la desinformación

Tomando en consideración las habilidades digitales presentadas en el apartado anterior, un tema de suma relevancia relacionado con la alfabetización digital es la existencia de la desinformación en Internet. De acuerdo a la Relatoría Especial para la Libertad de Expresión (RELE) de la CIDH, a través de su Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, en términos prácticos y provisorios, como la difusión masiva de información falsa:

a. con la intención de engañar al público, y
b. a sabiendas de su falsedad.

Si bien este fenómeno no es nuevo, los desarrollos tecnológicos recientes han hecho posible que se replique de forma acelerada, alcanzando a una mayor cantidad de personas y con consecuencias en diversas esferas de la vida pública[6]. De igual forma, la existencia de la desinformación pone en manifiesto la necesidad de desarrollar la habilidad de evaluar información de forma crítica, ya que si la información carece de autoridad, credibilidad y propósito, y se propaga de la misma forma, sus impactos pueden ser considerables.

La RELE, en esta misma guía, enfatiza el impacto que puede tener la desinformación en contextos electorales. Por ello, delinea una serie de recomendaciones para los diferentes actores participantes de los mismos. Estas se enfocan en ayudar a las partes involucradas a abordar problemas de desinformación, sin olvidar posibles efectos secundarios que podrían afectar negativamente estándares de derechos humanos.

Algunas de estas recomendaciones en materia de desinformación en el contexto de procesos electorales[7], que se centran en gran medida en la necesidad de aportar a la alfabetización y la seguridad digital, son:

6 Organización de los Estados Americanos. (2019). Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales. http://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf
7 La lista completa de recomendaciones puede encontrarse en la Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, páginas 30-51.

Para los Estados, incluyendo a los diferentes poderes públicos y autoridades electorales:

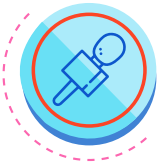
- Evitar establecer marcos regulatorios que responsabilicen a intermediarios por contenidos producidos por terceros.
- Fortalecer los marcos legales de protección de datos personales.
- Recordar las responsabilidades especiales que tienen los altos funcionarios públicos en el ejercicio de su propia libertad de expresión.
- Realizar acciones positivas de educación, capacitación y concientización para la ciudadanía, a fin de fortalecer sus capacidades para desarticular campañas de desinformación en contextos electorales.

Para las empresas intermediarias:

- Dar a conocer los criterios que se utilizan para moderar, detectar y priorizar contenidos en las plataformas y garantizar el debido proceso en la moderación de contenidos.
- Apoyar al periodismo de calidad y otras acciones positivas tendientes a contrarrestar las campañas de desinformación, incluyendo la colaboración con autoridades electorales y con investigadores independientes.
- Respetar y cumplir de forma proactiva la protección de datos personales.

Para los partidos políticos:

- Evitar campañas que utilicen información falsa.
- Transparentar la campaña electoral.
- Respetar y cumplir de forma proactiva la protección de datos personales.



Para los medios de comunicación y periodistas

- Fortalecer el periodismo de calidad frente a la desinformación.

Para los verificadores o *fact-checkers*

- Unificar definiciones de desinformación y fortalecer las redes regionales.

Para institutos académicos y de investigación

- Expandir las investigaciones empíricas sobre la desinformación.

A lo largo de esta guía, se abordan algunas nociones básicas sobre cómo fortalecer habilidades esenciales para lograr la alfabetización digital y combatir la desinformación y otros fenómenos que atentan contra su desarrollo digital seguro.

IMPORTANCIA DE LA ALFABETIZACIÓN DIGITAL PARA LA DEMOCRACIA

MISIÓN DE OBSERVACIÓN ELECTORAL DE LA OEA (DECO)

Las plataformas tecnológicas y las redes sociales han amplificado y creado nuevas modalidades de comunicación que han fortalecido la interacción entre representantes y ciudadanos, complementando con ello las formas más tradicionales de participación política. Ello ha contribuido a la generación de una ciudadanía activa e involucrada en el debate abierto en torno a las ideas e intereses que confluyen en el espacio público.

Actualmente se dispone de medios diversos para manifestar opiniones y posiciones propias, así como para informarse sobre los acontecimientos que ocurren en el entorno, ya sea a nivel municipal, departamental o nacional, o sobre sucesos que ocurren en otros países y continentes. Se tiene también la oportunidad de crear contenidos, los cuales pueden ser difundidos y compartidos con una amplia audiencia. Por otro lado, existe una interacción más directa con quienes ejercen funciones públicas, que no solo redunda en acceso sino también en fiscalización, posibilitando con ello que el ejercicio del poder esté hoy más que nunca sujeto a un escrutinio público constante e inmediato.

Ya es habitual acceder a las redes sociales de autoridades para informarse sobre el ejercicio de sus funciones, o de candidatas y candidatos para conocer sus propuestas en forma directa y mantenerse al día en torno a las actividades de campaña. Los partidos políticos se benefician al poder transmitir sus mensajes y visión política directamente a la ciudadanía a través de los diversos medios disponibles, ampliando el ámbito territorial a un alcance nacional. Al mismo tiempo, la sociedad civil tiene hoy plataformas con alcance masivo para difundir sus acciones y conectar con las personas. Y, en general, la ciudadanía cuenta hoy con nuevas formas de organización que posibilitan expresiones colectivas.

Los aspectos anteriores permiten que el entorno digital sea un eslabón importante de los procesos democráticos y de las elecciones, contribuyendo al ejercicio de la libertad de expresión, al libre acceso a la información y a la libertad de asociación. Asimismo, promueve la transparencia y rendición de cuentas, entre otros elementos. Hacia el futuro, el impacto que tienen las plataformas digitales y otras tecnologías de la información en nuestras democracias será cada vez mayor. La pandemia de COVID-19 profundizó este proceso. Sin embargo, así como existen importantes beneficios, también existen diversos riesgos. La dinámica propia del mundo digital expone a todas las personas que utilizan Internet a fenómenos como la desinformación, la vulneración de datos personales, actividades ilegales, la influencia de actores externos en la política interna o en procesos electorales, entre otros elementos, que directa o indirectamente minan la confianza en nuestras democracias.

Para poder hacer uso en plenitud de las diversas oportunidades que brinda el mundo digital, así como para conocer, comprender y protegerse de los riesgos que presenta este entorno en el cual cada vez se está más involucrado, es importante que la alfabetización digital alcance a todas las personas.

Se trata de un elemento esencial para el fortalecimiento de la democracia, y es un proceso necesario para que todos quienes intervienen desde el ámbito público, actores sociales, grupos de interés, instituciones, los medios, la sociedad civil, los partidos políticos y la ciudadanía en general, tengan las capacidades y oportunidades de hacer uso de los instrumentos que se disponen hoy para contribuir desde la tecnología a una democracia activa y responsable.

Aprender a utilizar las herramientas tecnológicas, acceder a la información, deslindar información de desinformación, evaluarla, ser crítico en su análisis, distinguir las fuentes, proteger los datos, resguardar la privacidad, son algunas de las condiciones necesarias para reducir la brecha digital, propiciar una interacción segura con las tecnologías y educar para una ciudadanía consciente e informada.

CIBERSEGURIDAD Y AUTOCUIDADO DIGITAL

INTERNET HA SIDO UNA HERRAMIENTA QUE HA TRANSFORMADO Y DEFINIDO LA COMUNICACIÓN EN EL SIGLO XXI.

A través de sus múltiples utilidades, ha permitido que tanto individuos como organizaciones se conecten y comuniquen. A raíz de los diversos acontecimientos en los últimos años, tales como la pandemia de COVID-19 y la aceleración de los procesos de digitalización en todo el mundo, cada vez más personas se valen de Internet para mantenerse conectadas y compartir mensajes e información de índole personal, profesional y social en diferentes plataformas.

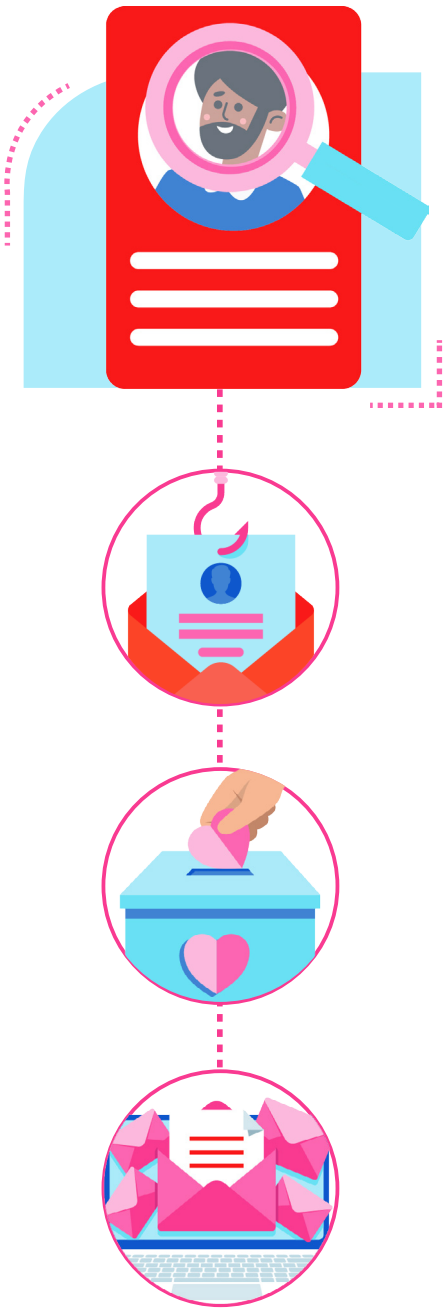
Sin embargo, a medida que se multiplican estos procesos, organizaciones e instituciones a nivel mundial han registrado un crecimiento considerable del nivel de exposición a riesgos en línea. Esto se debe principalmente a la falta de familiaridad con el uso a gran escala de las Tecnologías de la Información y la Comunicación (TIC) y a la carencia generalizada de conocimientos sobre ciberamenazas y herramientas de seguridad digital. Este bajo nivel de competencias de ciberseguridad, así como la exposición a más riesgos en línea, han configurado un escenario propicio para los atacantes, quienes han aprovechado la 'nueva normalidad' digital para explotar nuevas formas de ataque y acceso a datos personales (UNODC, 2020)[8].

Tomando en cuenta este escenario, esta sección ofrece una variedad de términos y descripciones para familiarizar al público general con estas formas de ataque que han cambiado a lo largo del tiempo. De igual forma, se incluyen consejos para mitigarlos y contrarrestarlos de forma proactiva.

8 Trend Micro. (2020). Developing Story: COVID-19 Used in Malicious Campaigns. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

¿Cómo reconocer ataques cibernéticos?

Si bien los ataques cibernéticos no son algo nuevo, es importante que exista una familiarización con los mismos para poder denunciar y actuar ante ellos.



Ingeniería Social

Características: La ingeniería social consiste en la utilización de métodos no tecnológicos para engañar a potenciales víctimas específicas que han sido previamente investigadas, para que compartan información personal sensible, como contraseñas o detalles de cuentas bancarias, de forma casi voluntaria con un hacker[9].

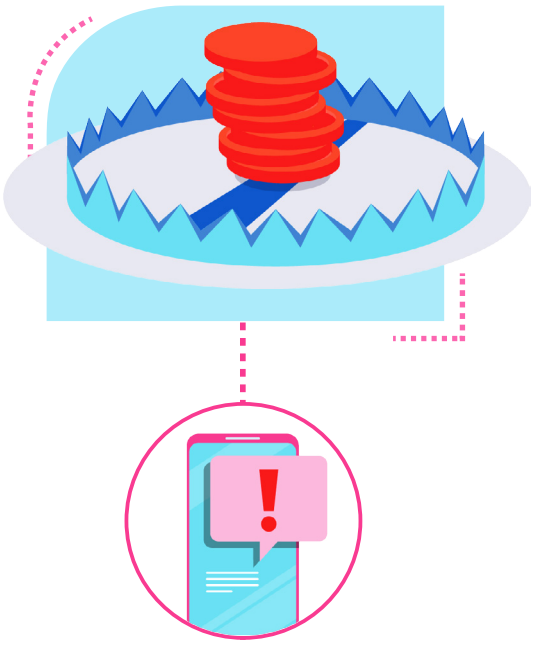
Algunos ejemplos son[10]:

Spear phishing: A través de la personalización de correos electrónicos, mensajes de phishing o suplantando la identidad de contactos cercanos, reclutadores, etc.
Ejemplo: un hacker que suplanta la información de un banco y pide a una persona información privada para "desbloquear su cuenta", o que se hace pasar por un reclutador para solicitar información de identidad para tramitar una oferta falsa.

Pretexting: A través de un pretexto o historia cautivadora, los hackers atraen la atención de una persona a quien se busca atacar y lo involucran para que haga alguna acción específica, como donar a una campaña falsa, o brindar información personal sensible.
Ejemplo: correos electrónicos en los cuales se promete dinero de una supuesta herencia, en la cual se busca obtener detalles de una cuenta bancaria.

Spam de contactos: Consiste en el envío masivo de correos electrónicos a una lista de contactos de una cuenta que ha sido hackeada. Estos correos se envían desde un buzón de correo conocido para no levantar sospechas, pero el contenido de los mismos aparecerá a los destinatarios con enlaces acortados o asuntos informales como "Mira esto". Si la persona hace clic, se instalará un software malicioso que continuará con esa cadena de spam y puede acarrear consecuencias negativas para sus datos personales.

9 NortonLifeLock. ¿Qué es la ingeniería social?. https://lam.norton.com/Internetsecurity-emerging-threats-what-is-social-engineering.html
10 SoftwareLab.org. ¿Qué es la ingeniería social?: La definición y los 5 ejemplos principales. https://softwarelab.org/es/que-es-ingenieria-social/



Fraudes, estafas por Internet y campañas de phishing

Características: Estos ataques se llevan a cabo de forma masiva a través de publicaciones o mensajes en redes sociales en los que información no verificada sobre temas que están en el ciclo de noticias se utiliza como señuelo, persuadiendo a los destinatarios para acceder a sitios web falsos, facilitar datos personales o bancarios o para infectar sistemas informáticos y dispositivos electrónicos[11].

Ejemplo: son comunes las campañas de phishing en las que los ciberdelincuentes suplantan la identidad de organismos internacionales y autoridades gubernamentales y sanitarias ofreciendo información o el apoyo de supuestos programas sociales[12] , invitando a hacer donaciones para responder a emergencias sanitarias, o, ante el incremento exponencial de las compras en línea, en las que se hacen pasar por servicios de paquetería o entrega a domicilio.

Las estafas circulan también a través de campañas de *smishing*, las cuales ofrecen alimentos gratuitos, bonos, productos médicos, descuentos, servicios gratuitos de recargas y suscripciones a plataformas de entretenimiento.

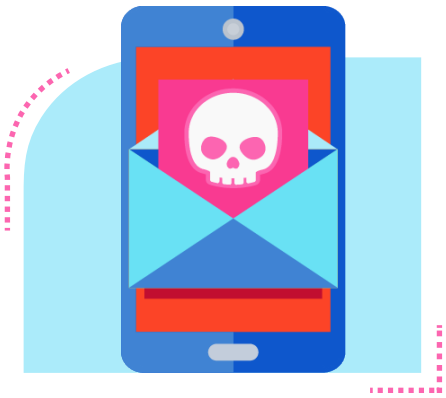
Malware o Instalación de software malicioso

Características: El *malware* o infiltración de contenido malicioso utiliza como señuelo información relacionada con temas relevantes en el ciclo de noticias para infiltrarse en dispositivos electrónicos. En el caso de América Latina, una amenaza recurrente durante años recientes han sido ataques de *ransomware* en contra de computadoras personales y teléfonos móviles, mediante los cuales los cibercriminales cifran y 'secuestran' información y datos personales de las víctimas exigiendo un rescate para desbloquear el equipo o la información captiva y liberar la información[13]. En ocasiones, los hackers también pueden incurrir en amenazas en contra de sus objetivos en caso de que estos se nieguen a pagar la recompensa esperada.

11 Porter, Taryn. (2020). COVID-19 Scam Alters. Cybercrime Support Network. https://cybercrimesupport.org/covid-19-scam-alerts/
12 Organización Mundial de la Salud. (2020). WHO reports a fivefold increase in cyber attacks, urges vigilance. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance; BBC News Mundo. (2020). Coronavirus: la advertencia de la OMS sobre los estafadores que están usando el nombre de la organización para robar dinero y datos. https://www.bbc.com/mundo/noticias-52009138
13 We Live Security y eset. (2020). Informe de Amenazas. Segundo Trimestre de 2020. https://www.welivesecurity.com/wp-content/uploads/2020/08/Q2-2020_Threat_Report-ESP.pdf

Creación de sitios web falsos *(spoofed domains)*

Características: En este caso, los ciberdelincuentes registran nombres de dominio con palabras clave que generalmente están asociadas a temas novedosos o de interés público para confundir a las personas. Esto se realiza con el fin de que las personas accedan a estas páginas en las cuales se ofrecen productos que prometen solucionar algún problema puntual con soluciones "milagrosas" o rápidas, pero en realidad se insertan softwares maliciosos o se pide algún tipo de información.



Mensajes de sextorsión falsos

Características: A través de este tipo de ataques, los hackers envían mensajes a las personas en los cuales amenazan con enviar a sus contactos vídeos íntimos y comprometedores que han obtenido al infiltrarse en sus dispositivos[14] o grabado mientras navegaba por páginas de contenido sexual. Esto por lo general viene acompañado de una notificación de pago de una cantidad monetaria exigida en una cartera digital, a cambio de evitar que se cumplan las amenazas presentadas por el hacker[15].

Ataques a través de las herramientas de trabajo remoto

Características: La pandemia por COVID-19 provocó que muchas empresas tengan una sucursal en cada hogar de sus empleados, quienes se están exponiendo a más riesgos en línea y, a su vez, exponen los sistemas informáticos de sus centros de trabajo. En este entorno, los ciberdelincuentes han identificado vulnerabilidades de software, redes y herramientas de trabajo remoto, dirigiendo ataques para infiltrarse en los sistemas corporativos a través de las computadoras personales de empleadas y empleados.

14 Ducklin, Paul. (2020). Dirty little secret extortion email threatens to give your family coronavirus. Sophos https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/
15 INCIBE y OSI. (2020). Detectada oleada de falsos correos de sextorsión o infección de COVID19. https://www.osi.es/es/actualidad/avisos/2020/04/detectada-oleada-de-falsos-correos-de-sextorsion-o-infeccion-de-covid19

Difusión de información falsa y desinformación

Características: La circulación de información falsa, no verificada o de teorías de conspiración en Internet facilita la ejecución de ciberestafas y otros ciberataques[16]. Esta información puede provenir de diversas fuentes, no solo de cuentas falsas, trolls o bots, sino también de cuentas oficiales y contactos cercanos y circula en Internet debido a que, en gran parte, la población la comparte de forma irreflexiva[17].

Uso del *Dark Web* para actividades criminales

Características: Se ha incrementado el uso de la *Dark Web* para la venta de información y datos personales o corporativos obtenidos vía *ransomware* y otras actividades maliciosas, incluyendo la explotación sexual infantil, la venta de datos personales o direcciones de correo, entre otras actividades ilícitas.

Medidas prácticas para hacer frente a los ataques cibernéticos

Ante las amenazas expuestas, este apartado pretende compartir pasos simples y sencillos para proteger información, cuentas y datos personales y corporativos ante ataques cibernéticos. Es importante destacar que estas recomendaciones se dirigen al público general y algunas pueden no ser aplicables a figuras públicas como políticos, activistas u otros actores cuyas prácticas de redes sociales están sujetas a un mayor escrutinio. Asimismo, el ejercicio de los derechos de expresión, reunión y protesta debe ser respetado en el ámbito digital al tiempo que garantice prácticas más seguras de Internet.

16 Stone, Jeff. (2020). How scammers use fake news articles to promote coronavirus 'cures' that only defraud victims.Cyberscoop. https://www.cyberscoop.com/coronavirus-cure-scam-social-media-riskiq/
17 NewsGuard. https://www.newsguardtech.com/

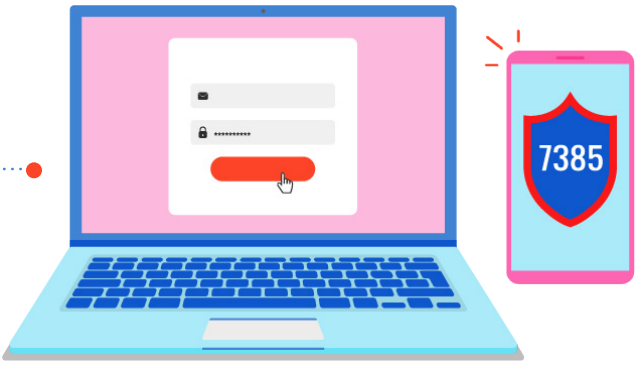
1. Revisar la configuración de privacidad

Administrar la configuración de privacidad en redes sociales y demás cuentas personales es una de las formas más simples a través de las cuales las personas pueden controlar la seguridad y privacidad de sus dispositivos y datos. A continuación, se presentan una serie de recomendaciones:

- Revisa regularmente la sección de “Privacidad” dentro de las configuraciones de tus cuentas de redes sociales, correo electrónico y dispositivos conectados a Internet.
- Selecciona quién tiene la capacidad de ver tu actividad en redes sociales (por ejemplo: tus Tweets e interacciones).
- Revisa si tu perfil se encuentra fácilmente accesible o público a otras personas y cómo pueden conectar contigo, ya sea mediante solicitudes de amistad o comenzando a “seguirte” en Twitter.
- Revisa, comprende y determina la cantidad de información personal que publicas en línea. Recuerda no colocar números de teléfono, claves personales o información sensible en publicaciones de tus redes sociales.
- Monitorea periódicamente la seguridad y la información de inicio de sesión de tus cuentas y revisa que no haya alguna actividad sospechosa, así como los permisos de aplicaciones de terceros que puedan estar accediendo a tus datos personales.
- Revisa la política de privacidad de la plataforma para saber qué datos recopilan los servicios, con quién(es) se comparten y selecciona tus preferencias en estos dos temas.

2. Configurar una autenticación de dos factores para iniciar sesión en tus cuentas personales

La autenticación de dos factores proporciona a las personas una capa adicional de seguridad, ya que requiere que las personas verifiquen su identidad con un segundo factor de verificación como la biometría (toma de huella dactilar o rostro) o proporcionando un código, protegiendo así del riesgo de credenciales débiles o comprometidas.



A continuación, se presentan las dos formas más conocidas para agregar esta capa de seguridad adicional, así como los pros y contras de cada una de ellas:

2 8 5 _ Método de doble autenticación	Pros	Contras
 **Mensaje de texto** Cada vez que la persona inicie sesión en una cuenta a través de un nuevo dispositivo, se le requerirá un código de varios números que se envía por mensaje de texto a su teléfono o por llamada telefónica.	• Esta es una forma sencilla de autenticar la identidad del usuario, ya que solo necesita un teléfono que pueda recibir mensajes de texto. • Es accesible, ya que en algunos casos el código también se puede enviar en forma de llamada.	• En casos de suplantación de identidad o pérdida o robo de su dispositivo móvil, otra persona podría obtener acceso a su información personal e iniciar sesión en sus cuentas. • Existe una práctica, llamada "portabilidad" o "sim swapping", la cual permite a un delincuente intercambiar la tarjeta sim del usuario por una infectada, para así interceptar los códigos de doble autenticación y acceder a cuentas personales.
 **Aplicación de autenticación de doble factor** Una aplicación de autenticación es una aplicación de software independiente que se descarga en un dispositivo móvil inteligente (tableta, iPad, etc.) o en una computadora. Esta genera un código aleatorio que se ingresa después de las credenciales o envía una notificación push (mensajes o alertas que se envían desde un servidor remoto hasta el dispositivos que tiene instalada una aplicación) para autenticar la identidad de la persona.	• Esta funcionalidad está disponible sin conexión a Internet. • No es susceptible a la portabilidad ya que no depende de un chip telefónico. • La versión de notificación automática ofrece el beneficio adicional de ser más rápida y fácil de usar. Si en la notificación aparece que la ubicación aproximada está lejos del hogar u oficina de la persona, es más probable que notificaciones como estas llamen su atención y lo estimulen a tomar las medidas necesarias.	• En el caso de que la aplicación envíe notificaciones push como método de autenticación, se requiere de conexión a Internet. • Si la persona extravía su teléfono o se apaga, y no tiene copias del código guardadas en otro lugar, no podrá acceder a la aplicación.

3. Gestionar la información personal incluida en el perfil

Al crear una cuenta en redes sociales, por defecto, toda la información divulgada en un perfil es pública, lo que significa que cualquier persona puede acceder al contenido publicado en esa cuenta. Sin embargo, las necesidades y preferencias de privacidad varían de persona a persona. Mientras que algunas personas prefieren tener una mayor exposición y así poder promocionar su contenido en redes sociales, otras prefieren incluir limitada o ninguna información. Para lograr una mayor protección, es importante evaluar en qué medida se está dispuesto a incluir información personal en un perfil. Por consiguiente, se recomienda tener en cuenta las siguientes configuraciones en las redes sociales:

Selección de nombre de usuario: el nombre de usuario es el "nombre digital" que una persona elige para ser identificada en línea como individuo u organización. Si la persona prefiere no ser fácilmente identificada, puede usar un seudónimo que puede estar relacionado o no con ella. Este nombre no tiene que ser consistente en todas las redes sociales y se puede cambiar en cualquier momento al ingresar a la configuración de la(s) cuenta(s).

Imágenes de cuenta: las personas tienen la opción de personalizar una cuenta con la inserción de una foto del perfil. Cuando las personas prefieren no ser identificadas, se sugiere elegir una imagen en la que no pueda ser reconocida y cambiarla cuando se considere necesario. La utilización de la misma imagen para todas las redes sociales facilita la identificación del usuario en las plataformas.

Inclusión de ubicación: Cuando se activan los servicios de ubicación en una plataforma de redes sociales, esto permite rastrear el origen de cualquier actividad de medios en línea. Es importante tener en cuenta que, una vez que se active esta función, permanecerá activa hasta que sea deshabilitada en la configuración de privacidad. Aunque una persona active o desactive la función de compartir su ubicación, potencialmente la misma podría ser descubierta a través del contenido o las imágenes que comparta.

Publicación de fotos: Las fotografías y otros archivos multimedia contienen información llamada data Exif, la cual detalla la ubicación, dispositivo, fecha y hora de captura, etc. Por ello, es importante conocer las políticas de privacidad de contenido multimedia de los sitios que visitas y donde compartes fotos, así como estar en constante alerta de con quién estás compartiendo tus publicaciones y contenido multimedia[18].

18 Germain, Thomas.(2019). How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.Consumer Reports.https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

4. Recomendaciones generales

El trabajo remoto o teletrabajo aumenta los riesgos asociados al manejo de información sensible en entornos corporativos y personales. Por ello, se recomienda tomar en cuenta los siguientes consejos adaptados a la "nueva normalidad" del teletrabajo y la vida digital[19]:

Mantener los softwares actualizados: Se recomienda que el software de todo dispositivo y aplicación se actualice con la mayor frecuencia posible. Esto le proporciona al usuario una mejor seguridad y velocidad de respuesta de su dispositivo. Asimismo, esto puede brindar protección contra estafas, virus, troyanos, ataques de phishing (suplantación de identidad), entre otras amenazas. Es probable que, con estas actualizaciones, las preferencias de privacidad se restablezcan, por lo que se recomienda que, cuando se realicen estas actualizaciones, se haga una revisión de la información que se comparte con aplicaciones y dispositivos móviles.

Utilizar un antivirus: El uso de software antivirus para dispositivos portátiles conectados a Internet sirve como un escáner inicial de cualquier actividad sospechosa o maliciosa a las que todo cibernauta está expuesto. Esto puede ayudar a supervisar la entrega de notificaciones y ofrecer un nivel adicional de protección en el evento que una persona haga clic erróneamente en enlaces sospechosos que pueden contener spam y diferentes tipos de virus.

Bloquear y filtrar: El uso de las funciones de bloquear, denunciar y la utilización de filtros para correos, mensajes y notificaciones permite que los servicios de las plataformas permanezcan seguros y resistentes. Cada vez que se bloquea una cuenta o una publicación, esto le da una señal importante a las plataformas sobre contenido o interacciones no deseadas para la persona, por lo que ese tipo de contenido se limita o bloquea. Es recomendable no ignorar un contenido sospechoso o que viole las políticas de uso de una plataforma: es mejor denunciarlo de manera continua. Si es necesario, también se debe denunciar amenazas que atenten contra su seguridad física a agentes del orden público[20].

Utilizar una computadora portátil de la empresa para el trabajo remoto si es posible y no compartir la información con otros miembros de tu hogar: No utilices tu máquina personal, ya que puede tener menos controles de seguridad que el hardware de su empresa. Si no puedes evitar el uso de equipos personales y tienes que utilizar tu propio dispositivo, mantente lo más cerca posible de los estándares de ciberseguridad de tu organización. Utiliza el software de seguridad proporcionado por tu empresa, sigue las medidas de protección de datos de la empresa y no mezcles tu uso personal con el laboral.

Utilizar VPN designadas y evitar las redes Wi-Fi públicas y gratuitas: La utilización de redes Wi-Fi públicas puede poner en riesgo información sensible como contraseñas, datos bancarios, entre otros. De igual forma, si se trabaja en un entorno corporativo, es recomendable hacer uso del VPN *(Virtual Private Network*, en inglés) designado para que los activos laborales se mantengan seguros mientras se trabaja desde un lugar remoto.

Utilizar redes divididas: Al trabajar en casa, es recomendable que la red personal sea de acceso propio y que se cree una red específica para el uso de invitados. Si tienes un enrutador o conmutador *(router)* con una funcionalidad (VLAN), actívalo y dedica una VLAN solo para temas de trabajo.

19 Roesler, Martin.(2020). Working From Home? Here's What You Need for a Secure Setup.Trend Micro. https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup

20 U.S. Department of Homeland Security. (2019). Social Media Plan Guide: Science and Technology Directorate. https://www.dhs.gov/sites/default/files/publications/social_media_plan_guide_09_20_2019.pdf

Preparar una solución de respaldo en casa: Tener opciones de respaldo (por ejemplo, hardware tales como discos duros externos o USB) es una medida preventiva clave en el caso de experimentar alguna falla en el almacenamiento de información como pérdida de conectividad o falla del servidor.

Reconocer los ataques de ingeniería social: Hay varias señales de alerta que pueden indicar un ataque de ingeniería social. Entre ellas, las más comunes son[21]:

Lenguaje genérico y con faltas: Si el correo proviene de una fuente segura y confiable, el cuerpo debe estar escrito de manera correcta según las reglas de ortografía y gramática. De lo contrario, es posible que se trate de un ataque. Otro elemento lingüístico que puede indicar un intento de ataque son los saludos y las formulaciones genéricas. Entonces, si un correo electrónico comienza con "Estimado destinatario" o "Estimado usuario", ten cuidado.

Remitente desconocido o con una identificación sospechosa: Si un correo electrónico proviene de una dirección que es una combinación de números y caracteres aleatorios o es desconocida para el destinatario, debe ir directamente a la carpeta de correo no deseado. Sin embargo, en algunos casos, los hackers también pueden tener una dirección de correo legítima, por lo que de todas formas es importante revisar las otras señales de alerta incluídas en este apartado.

Sentido de urgencia: Los delincuentes detrás de las campañas de ingeniería social a menudo intentan asustar a las víctimas para que actúen utilizando frases que provocan ansiedad como "envíenos sus datos de inmediato o su paquete será descartado" o "si no actualiza su perfil ahora, cerraremos su cuenta". Los bancos, las empresas de paquetería, las instituciones públicas e incluso los departamentos internos suelen comunicarse de forma neutral y objetiva. Por lo tanto, si el mensaje intenta presionar al destinatario para que actúe rápidamente, probablemente sea una estafa maliciosa y potencialmente peligrosa.

21 Eset. Social Engineering (in cybersecurity). https://www.eset.com/int/social-engineering-business/

Solicitud de información personal y privada: Las instituciones e incluso otros departamentos de su propia empresa normalmente no solicitarán información confidencial por correo electrónico o por teléfono, a menos que el contacto haya sido iniciado por el empleado.

Las anteriores son solo algunas recomendaciones a través de las cuales una persona u organización puede ser proactiva para garantizar altos niveles de ciberseguridad en las redes sociales y dispositivos electrónicos. Sin embargo, así como con la alfabetización, es responsabilidad de cada persona el mantenerse informada y revisar la configuración de privacidad, así como continuamente actualizar sus medidas de ciberseguridad para asegurar que sus datos e información importante se encuentre protegida en todo momento.

Conocer y poner en práctica este conocimiento y medidas de seguridad ayuda a las personas a estar mejor preparadas para, al momento de estar en línea, investigar, consumir y distribuir información de forma responsable. La siguiente sección indaga más a profundidad en estas áreas al usar Twitter como herramienta para mantenerse informado.

RECOMENDACIONES GENERALES PARA PERIODISTAS

Si bien las secciones anteriores contienen información clave para todas las personas, aquellas que se dedican a labores periodísticas, al igual que las demás personas que utilizan el internet para diferentes actividades, no están exentos de practicar buenos hábitos de seguridad digital para protegerse a la hora de ejercer su labor. Para estas personas, Internet también se ha convertido en una herramienta crucial para para desempeñar su rol, sobre todo en momentos clave de alto interés como lo son los procesos electorales en los que la información de un hecho noticioso se mueve a rápida velocidad. En este sentido, a continuación se presentan una serie de recomendaciones de ciberseguridad para momentos específicos, tomadas de la Guía de seguridad periodística para elecciones desarrollada por el Comité para la Protección de Periodistas (CPJ por sus siglas en inglés)[22]:

I. Preparación básica de dispositivos

Antes de salir a la cobertura, son buenas prácticas:

- Hacer copias de los datos de los dispositivos en un disco duro y borrar cualquier dato delicado del dispositivo que llevará.
- Cerrar las sesiones de todas las cuentas, las aplicaciones y los navegadores, así como borrar la historia de navegación.
- Proteger todos los dispositivos con contraseñas y configurar los dispositivos para que usted pueda borrar los datos de manera remota.
- Llevar la menor cantidad de dispositivos que sea posible. Si tienes dispositivos que no usas, llevarlos esos en lugar de sus dispositivos personales o de trabajo.

22 Forbes, Jack. (2019). Guía de seguridad periodística para elecciones. Comité de Protección de Periodistas. https://cpj.org/es/2019/10/guia-de-seguridad-periodistica-para-elecciones/#harassed

II. Cómo proteger y almacenar materiales informativos

Durante los períodos electorales, es importante disponer de buenos protocolos para almacenar y proteger materiales informativos. Si las autoridades detienen a un periodista cuando cubre una campaña electoral, ellas pudieran confiscar e inspeccionar los dispositivos del periodista y ello pudiera tener graves consecuencias para éste y sus fuentes informativas. Las siguientes medidas pueden ayudar a protegerse a sí mismo y a la información en su poder:

- Revisar la información almacenada en sus dispositivos, especialmente teléfonos y computadoras. Esto se realiza respaldando adecuadamente la información que pueda poner en riesgo o que contenga información delicada, y posteriormente borrar esa información del dispositivo.
- Revisar el contenido de sus teléfonos, incluyendo la información guardada en el teléfono (el hardware), al igual que la información guardada en la nube (Google Photos o iCloud).
- Revisar el contenido de las aplicaciones de mensajería, como WhatsApp. Guardar y luego borrar toda información que genere riesgo. Los trabajadores de medios deben tener en cuenta que WhatsApp hace una copia de respaldo de todo el contenido en el servicio en la nube vinculado con la cuenta, por ejemplo, iCloud o Google Drive.
- Retirar material informativo de sus dispositivos periódicamente y guardarlo en la opción para copias de respaldo de su preferencia. Ello asegurará que, si el dispositivo es confiscado o robado, aún conserven una copia de la información.
- Encriptar toda la información respaldada es beneficioso para mantener datos sensibles seguros. Esto se puede hacer encriptando el disco duro externo o el USB. También se puede activar la encriptación de dispositivos. Los periodistas deben estudiar la ley vigente en el país donde trabajan, para asegurarse de estar al tanto de los aspectos legales que rigen el uso de la encriptación.
- En casos de amenaza o riesgo de robo de dispositivos y discos duros externos, almacenarlos en un lugar físico diferente al domicilio.
- Bloquear todos los dispositivos con un PIN: mientras más largo sea el PIN, más difícil será descifrar.
- Configurar el teléfono o la computadora para poder borrarlos de manera remota. Esta es una función que le permite borrar los dispositivos a distancia, por ejemplo, en caso de que las autoridades u otros actores confisquen los dispositivos.

DISTRIBUCIÓN Y CONSUMO DE INFORMACIÓN EN TWITTER

Mantenerse seguro en línea es una práctica tan fundamental para tener una experiencia positiva y saludable en Internet, así como lo son el pensamiento crítico y uso de herramientas para la verificación de información. El funcionamiento de Twitter se basa en lo que está pasando y de lo que las personas están hablando en este momento, por lo que se ha convertido en la principal plataforma de información para muchas personas. Sin embargo, con tanta información disponible, a veces puede ser complicado seguir el ritmo de la conversación y verificar la veracidad de la información que se consume. La siguiente sección ofrece recomendaciones, herramientas y mejores prácticas para buscar, organizar, compartir y publicar información en Twitter.

Verificación de información en Twitter

En Twitter, las personas pueden hallar información y verificar su exactitud de manera rápida. Al ser una plataforma abierta y pública, existen diversas formas y herramientas para entablar conversaciones con otras personas o hacer una búsqueda rápida de un *hashtag*[23] o palabras claves, para evaluar la veracidad de la información que se consume en la plataforma.

Cuando se lee una información, es importante tener en cuenta los prejuicios propios y opiniones, al igual que las reacciones personales. A menudo, cuando se recibe información con la cual no se está de acuerdo, naturalmente las personas se hacen ciertas preguntas o comentarios que ayudan a desmentir dicha información. Sin embargo, generalmente se omite este escrutinio cuando lo que se lee confirma ideas preconcebidas. Ante este escenario, es importante adquirir la costumbre de siempre preguntarse quién, qué, dónde, cuándo, cómo y el porqué de una información antes de compartirla, hacer un Retweet[24], un Tweet con comentario, o darle un Me gusta.

23 Hashtags o etiquetas (escritos con el signo "#" antepuesto) se usan para indexar palabras clave o temas en Twitter. Esta función es una invención de Twitter y permite que las personas puedan encontrar fácilmente contenido alrededor de los temas que les interesan.
24 Un Retweet es la acción de compartir un Tweet ya existente.

Quién

- ¿Quién es la fuente? ¿La conoces?
- ¿Es una cuenta verificada?
- ¿A quién sigue y quiénes siguen a esta cuenta?
- ¿Quién escribe el artículo y cuál es su nivel de conocimiento del área?

Cuándo

- ¿Cuándo lo dijeron?
- ¿Cuándo se publicó? ¿Tiene fecha?

Qué

- ¿Qué dijeron?
- ¿Qué motivos tienen para compartir esta información?
- ¿Qué tipo de artículo es: información u opinión?
- ¿Qué tono están utilizando? ¿Es, quizás, intencionalmente falsa o una broma?
- ¿Qué respuestas está recibiendo este contenido? Es decir, ¿qué dicen las personas en Twitter?

Por qué

- ¿Por qué se publicó la noticia?
- ¿Es para generar tráfico el sitio web o cuenta?
- ¿Es para provocar una acción? En caso afirmativo, ¿de quién y para qué?

Dónde

- ¿Dónde ocurrió?
- ¿Dónde lo dijeron o publicaron?
- ¿Es una fuente fiable?
- ¿Cuál es el URL o enlace del sitio web? ¿Es legítimo?
- ¿Qué otros medios o personas cubrieron esta noticia?

Cómo

- ¿Cómo está escrito?
- ¿Tiene un exceso de signos de puntuación y letras mayúsculas para hacerlo sensacionalista?
- ¿Tiene un titular engañoso?
- ¿Está utilizando hashtags no relacionados al tema para llamar la atención?
- ¿Tiene un tono conspirativo?

A primera vista parecen ser muchas preguntas, pero estas pueden ser respondidas en cuestión de segundos y hay herramientas de Twitter que facilitan esta tarea y favorecen en gran medida el consumo seguro e informado de información en la plataforma. En el siguiente apartado se exponen dichas herramientas así como consejos para su uso.

Herramientas de Twitter para mejorar el consumo de información

Twitter continúa desarrollando actualizaciones de producto para ayudar a las personas a encontrar información y conocer el contexto alrededor de la misma de una manera fácil y rápida. Por ejemplo, para ayudar a las personas a mantenerse informadas sobre importantes eventos nacionales y globales, algunas veces se muestra en la cronología información confiable y de alta calidad sobre eventos que son de gran interés público como información sobre elecciones, desastres naturales, o crisis globales como COVID-19, y se le permite a las personas seleccionar si desean continuar viendo esa información o si no es de su interés.

Por otro lado, para ayudar a las personas a conocer el contexto alrededor de una información, cuando las personas quieren retwittear (compartir) un Tweet que contiene un enlace que no ha sido abierto por la persona desde la plataforma, Twitter empuja un aviso que recomienda a las personas abrir dicho enlace para conocer toda la información antes de compartirlo. Esto anima a las personas a hacerse preguntas críticas sobre la información que están por compartir.

Los anteriores son ejemplos de producto que ayudan a las personas a estar mejor informadas de forma reactiva. Además de esto, existen herramientas de Twitter y otros elementos en el diseño de la plataforma, que ayudan a las personas a explorar y organizar proactivamente la gran cantidad de información disponible en la plataforma, y añaden contexto adicional a la misma para su análisis y verificación. Algunas de estas son:

Las Tendencias existen para ayudar a las personas a descubrir conversaciones que se están desarrollando a su alrededor. Estas se determinan automáticamente, tomando en cuenta diferentes factores para identificar temas que gozan de popularidad en un momento dado, en lugar de temas que han sido populares durante un tiempo o diariamente.

Las Tendencias están disponibles en la aplicación de Twitter en la sección de ***Explorar*** , y en twitter.com en diferentes lugares, como en la cronología de inicio, las Notificaciones, los resultados de búsqueda y las páginas de perfil. Al pulsar o hacer clic en cualquier tendencia, verás los resultados de búsqueda de Twitter relacionados con esa tendencia, es decir, todos los Tweets que incluyan esa frase o hashtag.

Tendencias para ti vs. Tendencias de una ubicación geográfica

De forma predeterminada en Twitter se muestran las Tendencias *Para ti*, las cuales se determinan automáticamente tomando en cuenta las cuentas que sigues, tus intereses y tu ubicación. Para ver las Tendencias según un área geográfica, en twitter.com o desde la aplicación, puedes hacer clic en el icono de ***Configuración*** y seleccionar Tendencias de ubicaciones específicas. Si no encuentras la ciudad o el país que buscas, significa que aún no hay suficientes Tweets en esa zona geográfica para crear una lista de Tendencias. En estos casos, se pueden buscar Tweets locales sobre cualquier tema utilizando la Búsqueda Avanzada de Twitter.

Contexto en las Tendencias

Junto con algunas Tendencias, puede verse:

- El número aproximado de Tweets asociados a dicha tendencia. Es importante entender que el número de Tweets relacionados con las Tendencias es solo uno de los factores que se toman en cuenta a la hora de clasificar y determinar las Tendencias. Por eso a veces se puede ver que el número de Tweet de las primeras Tendencias es menor al número de Tweets de las siguientes.
- Información contextual personalizada, por ejemplo, quiénes en tu red de contactos están twitteando sobre la tendencia.
- Una categoría como “Política”, “Música” o “Entretenimiento”. Esto se selecciona automáticamente en función de lo que tratan los Tweets de la tendencia.
- Artículos, que se adjuntan automáticamente en función de la conversación sobre la tendencia.

Resultados de búsqueda

Cada vez que se hace una búsqueda en Twitter, bien sea desde twitter.com o desde la aplicación, los resultados pueden ser visualizados de acuerdo a cuándo fueron compartidos o al tipo de contenido. Es decir, cada búsqueda es organizada de forma automática en diferentes pestañas que dan la opción de ver los Tweets:

Destacados

Resultados más relevantes de acuerdo a los intereses de la cuenta que realiza la búsqueda.

Más recientes

Resultados de búsqueda en orden cronológico.

Personas

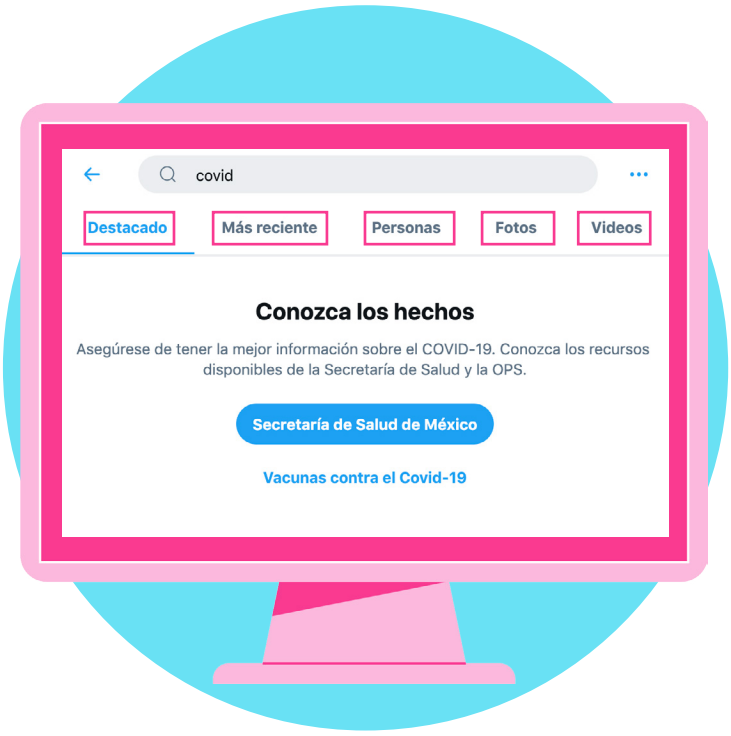
Resultados de las cuentas que coinciden con la consulta.

Fotos

Resultados de búsqueda que contienen fotos.

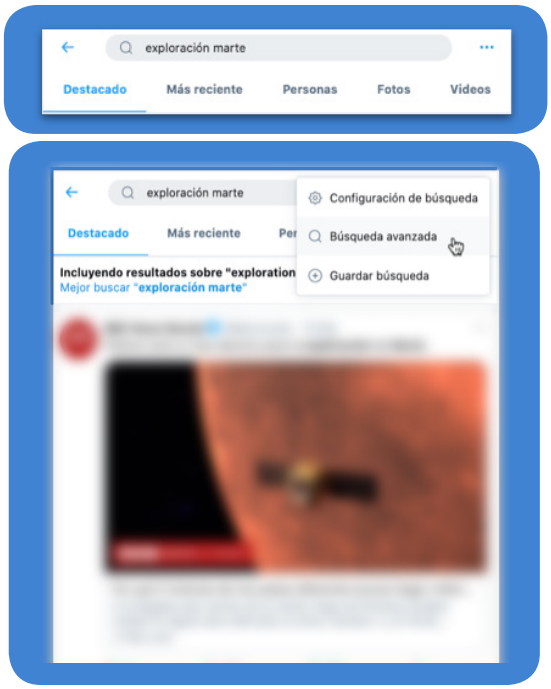
Videos

Resultados de búsqueda que contienen video.



Búsqueda avanzada

Si se quiere buscar alguna información precisa en twitter.com, existe la opción de realizar una búsqueda avanzada. Esta opción está disponible a través del menú desplegable para *más opciones* , en la parte superior de la página, y haciendo clic en Búsqueda avanzada. Allí se presentan una serie de campos mediante los cuales se puede refinar la búsqueda para encontrar contenido específico de una manera más directa y rápida.



En la aplicación, las opciones de búsqueda son más limitadas, pero, con ciertas fórmulas de búsqueda, también se puede refinar la información de los resultados. Utilizando la frase *Twitter app*, el siguiente ejemplo ilustra cómo se pueden utilizar algunas nomenclaturas de acuerdo al contenido que se busca:

Twitter app

para buscar contenidos que contengan todos los términos de búsqueda, sean palabras, @nombres de cuentas o hashtags. En este caso, la palabra *Twitter* y la palabra *app*.

Twitter -app

utilizando un guión, o símbolo de sustracción, para buscar contenidos que contengan la palabra *Twitter* pero no la palabra *app*. Es decir, que excluyan lo que se coloca después del guión.

"Twitter app"

para buscar contenidos que contengan exactamente la frase entre comillas, es decir, *"Twitter app"*.

from:TwitterSeguro

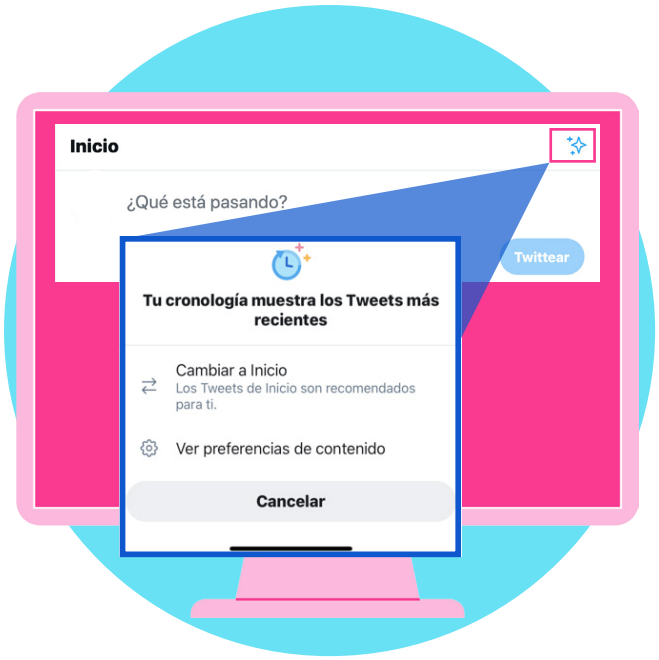
para buscar contenidos publicados desde una cuenta específica de Twitter. En este caso, *@TwitterSeguro*.

Twitter OR app

para buscar contenidos que contengan uno u otro término. En este caso, los términos *Twitter* o *app*, o ambos.

Cronología de Inicio: "Tweets destacados" vs. "Tweets más recientes"

La página principal de twitter.com o de la aplicación muestra, de forma predeterminada, los Tweets más relevantes en la parte superior de la cronología. Sin embargo, a veces es mejor ver los Tweets en orden cronológico, es decir, ver primero los Tweets más recientes. Esto no solo depende de las preferencias de cada persona, sino también de la información que se busca. Por ejemplo, durante un evento deportivo o en situaciones de emergencia, es más útil ver primero la información más actual.



Por ello, en Twitter existe la posibilidad de cambiar de forma fácil y rápida la configuración de la cronología de inicio entre Tweets destacados y Tweets más recientes. Para hacer este cambio, desde twitter.com o desde la aplicación, pulsa el ícono en la esquina superior derecha y elige la opción de preferencia.

La opción predeterminada en Twitter es la de Tweets destacados, así que cuando se cambia la configuración a Tweets más recientes y se deja de usar Twitter por un tiempo, la configuración se revertirá automáticamente a Tweets destacados.

Notificaciones de cuenta

Hay momentos en los cuales es necesario o deseado estar al tanto del contenido publicado por cuentas específicas y para esto existen las Notificaciones de cuenta o notificaciones push. Estas notificaciones envían al usuario un mensaje o alerta cuándo ciertas cuentas publican Tweets. Existe la opción de seleccionar activar estas notificaciones para todos los Tweets de una cuenta, o solo para los Tweets que contengan transmisiones en vivo. Estas se pueden activar o desactivar en cualquier momento.

Para activar las Notificaciones:

1. Asegúrate de estar siguiendo la cuenta para la cual quieres recibir notificaciones en tiempo real.
2. En el perfil de la cuenta, bien sea en twitter.com o en la aplicación, pulsar el ícono de *Notificación* .
3. Si haces esto desde twitter.com, se activarán ambas notificaciones: para todos los Tweets y para transmisiones en vivo. Desde la aplicación, existe la posibilidad de elegir entre dos tipos de notificaciones: *Todos los Tweets o Solo Tweets con video en directo.*

Para **cancelar las Notificaciones,** regresa al perfil de la cuenta, pulsa el ícono de *Notificación resaltado* y selecciona *Ninguna.*

Si es necesario revisar qué Notificaciones están activas, esto se puede ver hacerlo desde la aplicación en:

1. El menú de tu cuenta.
2. Selecciona *Configuración y privacidad.*
3. Pulsa *Notificaciones* y, luego, *Notificaciones push.*
4. Pulsa *Tweets.*

Listas

Una Lista es un filtro que muestra una cronología de inicio personalizada en la que únicamente aparecen los Tweets de las cuentas incluidas en esa Lista. Por ejemplo, se puede filtrar la cronología de inicio creando Listas específicas de de expertos, periodistas, comediantes, autoridades, servicios, etc. Algunas características importantes de las Listas incluyen:

- Existe la posibilidad de crear Listas propias o suscribirse a Listas creadas por otras personas.
- No es necesario seguir a una cuenta para poder agregarla a una Lista.
- Las Listas pueden ser privadas, para monitoreo personal, o públicas, para compartir información con otras personas.
- Si las Listas son públicas, las cuentas que se agregan a la Lista recibirán una notificación al respecto.
- En la aplicación, se pueden fijar hasta 5 Listas a la pantalla de inicio para accederlas de forma rápida.

Para crear una lista:

1. Haz clic en el ícono de tu perfil para abrir el menú desplegable.
2. Haz clic en *Listas*.
3. Haz clic en *Crear nueva Lista*.
4. Elige un nombre para tu Lista y escribe una descripción breve. En este paso debes indicar si la Lista debe ser privada (solo el dueño de la cuenta podrá verla y acceder a ella) o pública (cualquier persona puede ver y suscribirte a la Lista).
5. Haz clic en *Guardar Lista*.

Para agregar personas a una Lista:
Para realizar esto no es necesario seguir a las cuentas que se quieren agregar a la Lista.

1. Haz clic en el ícono de contenido *adicional* en el perfil de la cuenta que quieres agregar a la Lista.
2. Selecciona *Agregar o eliminar de las Listas*. Se abrirá una ventana emergente donde se muestran las Listas ya creadas o se da la opción de crear una nueva.
3. Haz clic en la/s Listas a la/s que deseas agregar la cuenta o quita la marca de las Listas de las que deseas eliminar la cuenta.

Editar o borrar una Lista:

1. Haz clic en el ícono de tu perfil para abrir el menú desplegable.
2. Haz clic en *Listas*.
3. Haz clic o pulsa la Lista que deseas editar o eliminar de las Listas que creaste.
4. Haz clic o pulsa el botón de *Editar* para actualizar los detalles de la Lista o para eliminar la Lista por completo.

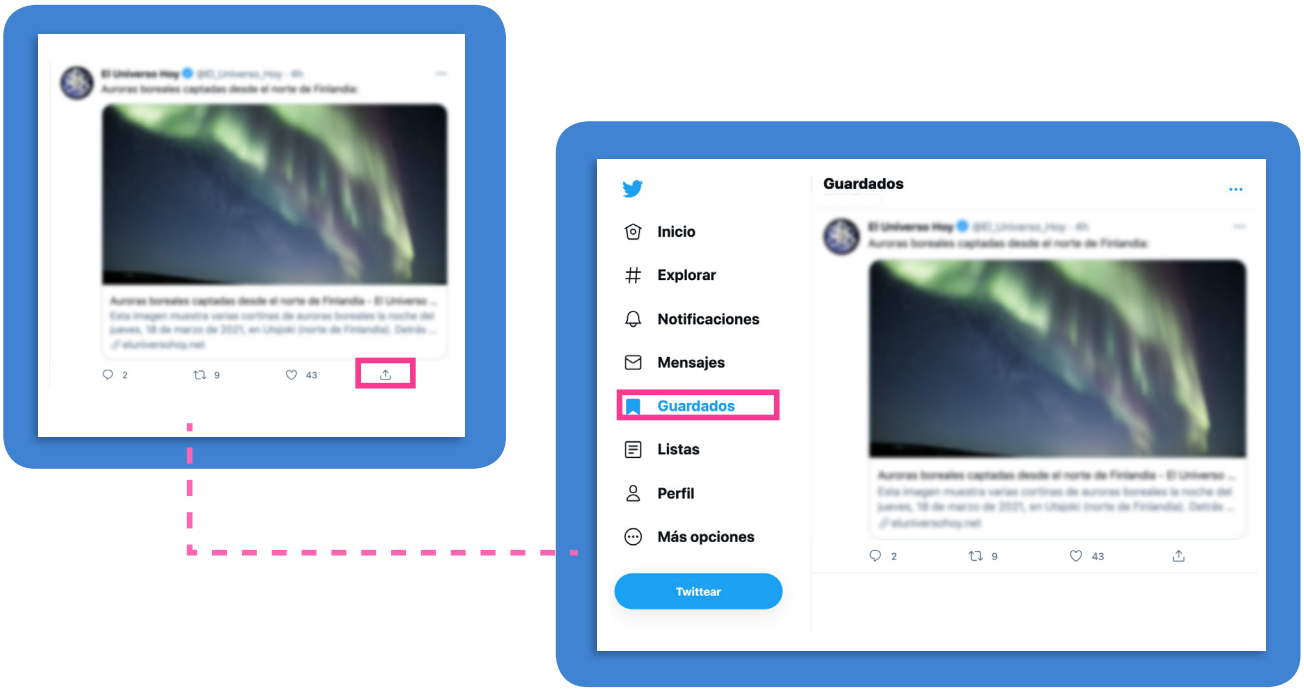
Suscribirse a Listas de otras cuentas:

1. Haz clic en el ícono de contenido *adicional* en el perfil de una cuenta.
2. Haz clic o pulsa la opción *Listas*.
3. Selecciona la Lista a la que deseas suscribirte.
4. En la página de la Lista, se puede hacer clic o pulsar la opción *Suscribirse* para seguir la Lista. Puedes seguir Listar sin tener que seguir a la cuenta que la creó ni tener que seguir a cada una de las cuentas que forman parte de la misma.

Tweets guardados (Bookmarks)

Desde artículos e Hilos, hasta vídeos y GIFs, la cronología de inicio está repleta de contenido para el que no siempre hay tiempo de explorar en el momento inicial en el que se encuentra, o que se quiere guardar para poder revisar o referenciar más adelante. Para estos casos existen los *Bookmarks* o Elementos guardados de Twitter.

Para marcar un Tweet como un Elemento guardado, pulsa el ícono de ***compartir*** que se encuentra debajo del Tweet que se desea guardar y selecciona *Agregar Tweet a Elementos guardados*. Cuando quieras localizarlo, pulsa *Elementos guardados* en el menú de tu perfil y allí los encontrarás. Los Tweets pueden ser eliminados del marcador en cualquier momento y sólo el dueño de la cuenta puede ver sus marcadores.



El uso adecuado de estas herramientas es clave para verificar la información que se encuentra en Twitter, pero estar en la plataforma implica mucho más que consumir información. También se trata de compartir información e interactuar con otras personas. Para garantizar que Twitter sea un espacio donde las personas pueden participar de manera libre y segura, existen reglas sobre lo que está y no está permitido en Twitter, así como herramientas para ayudar a las personas a controlar su experiencia en la plataforma. En la siguiente sección se exponen estos lineamientos.

MEJORES PRÁCTICAS EN TWITTER PARA AUTORIDADES Y ORGANIZACIONES

Twitter es una de las plataformas de redes sociales más rápida que tienen las organizaciones, autoridades y expertos para compartir información relevante y veraz con la mayor cantidad de personas y con un mínimo esfuerzo.

Para usar Twitter de manera efectiva, aumentar la credibilidad de su presencia en línea y posicionarse como fuentes de información confiable, las organizaciones, entidades, o autoridades deben tener un plan de contenido constante e interactivo, que refleje su credibilidad y relevancia. Algunos consejos para hacer esto posible:

- El perfil de la cuenta es tu carta de presentación en Twitter, por lo que debe reflejar la información más actualizada: nombre, biografía, ubicación, y sitio web. Igualmente, la foto de encabezado y de perfil ayudan a las personas a identificar fácilmente la identidad de la cuenta.

- Los mensajes siempre deben ser concisos, fáciles de digerir y tener un tono conversacional en lugar de pretender entablar un discurso. Las personas van a Twitter para interactuar, hacer preguntas, y compartir reacciones. Interacciones básicas como Me gusta, Retweets, menciones y respuestas pueden ayudar a desarrollar conversaciones alrededor de tus temas de interés.

- El contenido multimedia es sumamente interactivo y efectivo, pero solo si se comparte de forma nativa y no desde otras plataformas. También es importante que el contenido multimedia esté claramente relacionado con el mensaje que se quiere compartir, y en el caso de los videos, que sean sumamente cortos – 16 segundos es lo ideal.

- La relevancia del momento es clave en Twitter. Participar en el momento en el que ocurren los hechos, compartir reacciones y dar información de primera mano aumenta la relevancia y credibilidad de tu presencia en Twitter.

- Mantenerse conectado, motivar conversaciones, hacer sesiones de preguntas y respuestas – agrupadas alrededor de un hashtag – y transmisiones en vivo son importantes para compartir tu punto de vista único del momento de forma directa con tus seguidores para ayudarlos a estar mejor informados.

SEGURIDAD EN TWITTER

Twitter es un espacio abierto de libre expresión, en el cual todas las personas pueden participar libremente. Esto permite que sea una herramienta útil y relevante para compartir y encontrar información al día y de forma rápida. Para garantizar que las personas se sientan seguras al expresar diversas opiniones y creencias, existen reglas en el uso de la plataforma, a fin de cuidar la salud de la conversación pública y evitar que haya voces que sean silenciadas. En esta sección se explican las Reglas de Twitter, las cuales son importantes lineamientos para saber que está y qué no está permitido en la plataforma. También se describen las herramientas disponibles para personalizar y controlar la experiencia de cada persona en la plataforma para que sea lo más agradable y fructífera posible.

Reglas de Twitter

Twitter refleja las conversaciones reales que suceden en el mundo, y, a veces, eso incluye perspectivas que a algunos les pueden resultar ofensivas, controversiales o intolerantes. Si bien Twitter es un espacio participativo donde se pueden expresar opiniones diversas, en la plataforma no se toleran comportamientos que utilicen el acoso, la intimidación o el miedo para silenciar la voz de otras personas. Las reglas de la plataforma tienen como objetivo garantizar que todas las personas puedan participar en la conversación pública de manera libre y segura. Estas reglas están divididas en tres categorías principales: **seguridad, privacidad y autenticidad.**

Seguridad

- Violencia: No está permitido hacer amenazas violentas contra una persona o un grupo de personas. También se prohíbe la glorificación de la violencia.
- Terrorismo o extremismo violento: No está permitido amenazar o fomentar el terrorismo o el extremismo violento.
- Explotación sexual infantil: En Twitter existe cero tolerancia con respecto a la explotación sexual infantil.
- Abuso/acoso: No está permitido participar en situaciones de acoso dirigidas a una persona o incitar a otros a hacerlo. Esto incluye desear o esperar que alguien sufra daños físicos.
- Comportamientos de incitación al odio: No está permitido fomentar la violencia contra otras personas ni amenazarlas o acosarlas por motivo de su raza, origen étnico, origen nacional, pertenencia a una casta, orientación sexual, género, identidad de género, afiliación religiosa, edad, discapacidad o enfermedad grave.
- Suicidio y autolesiones: No está permitido fomentar ni promover el suicidio o las autolesiones.
- Contenido multimedia de carácter delicado, incluyendo la violencia gráfica y el contenido para adultos: No está permitido publicar contenido multimedia que sea excesivamente morboso ni compartir contenido violento o para adultos en videos en vivo o en imágenes de perfil o encabezados. El contenido multimedia donde se representa violencia o abusos sexuales tampoco está permitido.
- Bienes o servicios ilegales o regulados: No está permitido utilizar Twitter para ningún propósito ilegal o para promover actividades ilegales. Esto incluye la venta, compra o facilitación de transacciones de bienes o servicios ilegales, así como determinados tipos de bienes o servicios regulados.

Privacidad

- Información privada: No está permitido publicar la información privada de otras personas (como el número de teléfono y la dirección de su casa) sin su autorización y consentimiento. También está prohibido amenazar con divulgar información privada o incentivar a otros a hacerlo.
- Desnudez no consensuada: No está permitido publicar ni compartir fotos o videos íntimos de otra persona que se hayan producido o distribuido sin el consentimiento de esa persona.

Autenticidad

- Spam y manipulación de la plataforma: No está permitido usar los servicios de Twitter con el propósito de amplificar o suprimir información de forma artificial, ni llevar a cabo acciones que manipulen u obstaculicen la experiencia de las personas en Twitter.

- Integridad electoral: No está permitido utilizar los servicios de Twitter con el fin de manipular elecciones o interferir en ellas. Esto incluye publicar o compartir contenido que pueda disuadir la participación de los votantes o engañar a las personas sobre cuándo, dónde o cómo votar.

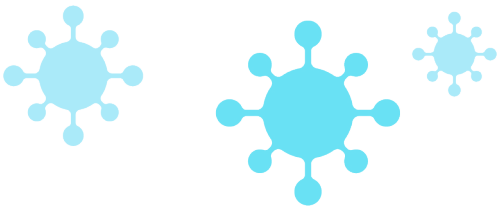
- Suplantación de identidad: No está permitido suplantar la identidad de otras personas, grupos u organizaciones de manera que intente, o logre confundir, engañar o comunicar una idea equivocada a otras personas.

- Contenidos multimedia falsos y alterados: Está prohibido compartir, con la intención de engañar, contenido multimedia falso o alterado que pueda dar lugar a daños graves. Asimismo, es posible que se etiqueten Tweets que incluyen contenido multimedia falso y alterado para ayudar a las personas a comprender su autenticidad y para ofrecer más contexto.

- Derechos de autor y de marca: No está permitido infringir los derechos de propiedad intelectual de otros, incluidos los derechos de autor y de marca.

Información más detallada sobre las Reglas de Twitter, así como la versión más actualizada de las mismas, está disponible en el Centro de Ayuda de Twitter o a través de: https://twitter.com/rules.

Se debe tener en cuenta que las Reglas de Twitter están en constante evolución y es posible que cambien ocasionalmente, a fin de respaldar el objetivo de fomentar una conversación pública saludable y constructiva. Tal fue el caso a raíz de la pandemia mundial de COVID-19 que ocasionó un cambio en las reglas para ampliar la definición de daño y abordar contenido directamente en contra de lo instruido por fuentes autorizadas de información de salud pública global y local. Estos procesos de actualización se hacen de forma transparente y comunicativa. Por ejemplo, durante los cambios realizados a raíz de COVID-19, Twitter mantuvo a las personas al tanto a través de su blog Coronavirus: Mantente Seguro e Informado en Twitter.



Aplicación de las Reglas de Twitter

Cuando Twitter toma medidas de aplicación de sus reglas, puede hacerlo en relación a un contenido específico (por ejemplo, un Tweet o Mensaje Directo), a una cuenta, o en combinación de estas opciones. En la aplicación de las reglas, Twitter parte del supuesto de que las personas no incumplen las reglas intencionalmente. Por ello, a menos que un incumplimiento resulte tan flagrante que obligue a la plataforma a suspender una cuenta de forma inmediata, primero se procura educar a las personas acerca de las Reglas de Twitter. Al hacer esto, Twitter le brinda a las personas que usan la plataforma la oportunidad de corregir su comportamiento, mostrándoles el o los Tweets que violan las reglas, explicando qué regla se incumplió y solicitando que se elimine el contenido para que la persona pueda poder volver a twittear. Si una persona incumple las reglas de forma reiterada, las medidas de aplicación de las mismas se tornan más serias.

Medidas a nivel del Tweet

Se toman medidas a nivel del Tweet para no ser excesivamente estrictos con una cuenta que cometió un error e incumplió las reglas pero que, por lo demás, no presenta problemas. Entre estas medidas se incluyen:

Limitar la visibilidad del Tweet

Esta medida reduce la visibilidad del contenido en Twitter, en los resultados de búsqueda, en las respuestas y en las cronologías.

Solicitar la eliminación del Tweet

Si se determina que el Tweet incumplió las Reglas de Twitter, se le solicita a la persona que cometió la infracción que lo elimine para poder volver a twittear. En estos casos, la persona recibe una notificación por correo electrónico en la que se identifica el o los Tweets que violan las reglas. El Tweet en cuestión deberá ser eliminado o la personas debe apelar a la decisión si considera que se cometió un error.

Ocultar un Tweet infractor mientras se elimina

En el período que transcurre entre que Twitter toma una medida de cumplimiento y la persona elimina el Tweet en cuestión, el Tweet se oculta para que el público general no pueda verlo y es reemplazado con un aviso que indica que el Tweet ya no está disponible porque incumple las Reglas de Twitter. Dicha notificación se mantiene durante 14 días después de la eliminación del Tweet.

Aviso de excepción de interés público

En casos muy específicos en los que se determina que es de interés público que un Tweet, que incumple las Reglas de Twitter, siga accesible en la plataforma, se coloca el Tweet detrás de un aviso que explica dicha excepción y da la opción de ver el Tweet si así lo desea la persona.

Al aplicar este aviso, también se toman medidas para reducir la visibilidad del Tweet, como:

- ✔ Desactivar las interacciones al Tweet (respuestas, Retweets y Me gusta).
- ✔ No mostrar ningún conteo de interacciones del Tweet (por ejemplo, cantidad de Me gusta o respuestas).
- ✔ Las respuestas anteriores que haya recibido el Tweet no son visibles.
- ✔ El Tweet deja de estar disponibles en:
    - La cronología de inicio bajo *Tweets Destacados.*
    - Los resultados de búsqueda.
    - Recomendaciones y Notificaciones.
    - La pestaña de *Explorar*.

En el siguiente apartado se explican más detalladamente los avisos en Twitter y su significado.

Medidas a nivel del Mensaje Directo

Detener las conversaciones entre una persona denunciada y la cuenta del denunciante

Cuando uno de los participantes de una conversación privada, es decir, por Mensaje Directo denuncia al otro participante, Twitter impide que la persona denunciada continúe enviando mensajes a la persona que lo denunció. Además, la conversación se elimina de la bandeja de entrada del denunciante y solo puede reanudarse si el denunciante decide seguir enviando Mensajes Directos a dicha persona.

Colocar un Mensaje Directo detrás de un aviso

En el caso de una conversación grupal por Mensaje Directo, es posible que el mensaje infractor se coloque detrás de un aviso para que nadie más en el grupo pueda volver a verlo.

Medidas a nivel de la cuenta

Twitter toma medidas a nivel de la cuenta si se determina que una persona incumplió las Reglas de Twitter de forma flagrante o que las incumplió reiteradamente incluso después de haber recibido notificaciones al respecto.

Solicitar la modificación de la información o del contenido multimedia del perfil

Si el perfil o el contenido multimedia de una cuenta no cumplen con las reglas, la cuenta puede ser suspendida temporalmente y Twitter, además de informar al dueño de la cuenta, puede solicitar que la persona modifique el contenido o la información de su perfil para que cumplan con las reglas.

Configurar una cuenta para que sea de solo lectura

Si una cuenta que, por lo demás, no presenta problemas, tiene un episodio de comportamientos abusivos, Twitter puede modificar temporalmente su configuración para que sea de solo lectura, limitando su capacidad de twittear, retwittear o usar la función Me gusta por un tiempo determinado. La persona afectada aún podrá ver su cronología de inicio y enviar Mensajes Directos a sus seguidores.

Cuando una cuenta está en modo de solo lectura, los demás pueden seguir viéndola e interactuando con ella. La duración de esta medida de control del cumplimiento puede variar entre 12 horas y 7 días, según el tipo de incumplimiento.

Verificar la titularidad de la cuenta

Para asegurar que las personas no abusen del anonimato que Twitter ofrece, en algunas oportunidades, Twitter solicita al titular de una cuenta que verifique su número de teléfono o dirección de correo electrónico para comprobar su autenticidad. Esto, entre otras cosas, ayuda a identificar y a tomar medidas con respecto a cuentas que son manejadas por una misma persona con fines abusivos.

Suspensión permanente

Esta es la medida más sería para garantizar la aplicación de las reglas. La suspensión permanente de una cuenta hace que esta se elimine de la vista a nivel global y la persona que cometió la infracción no podrá crear cuentas nuevas. Cuando se suspende una cuenta de forma permanente, se le informa a la persona acerca de la suspensión por incumplimientos relativos al abuso y se explica qué política o políticas incumplió y cuál fue el contenido infractor.

Apelaciones a estas medidas

Ante cualquiera de las acciones señaladas, las personas denunciadas o infractores pueden apelar a dichas medidas si consideran que Twitter ha cometido un error. Pueden hacerlo a través de la interfaz de la plataforma o mediante el envío de un informe desde el formulario de apelación.

Reportar violaciones a las Reglas de Twitter

Si al estar en Twitter encuentras contenido que consideras que viola alguna de las reglas de la plataforma, lo mejor que se puede hacer es reportarlo. Al reportar, recuerda que el contexto que puedas proporcionar es muy importante. De igual manera, ten en cuenta que no todo el contenido que algunos consideran ofensivo o intolerante está necesariamente en violación a las Reglas de Twitter.

A la hora de determinar si se tomarán medidas al respecto de un reporte, los equipos de Twitter consideran una serie de factores, entre los que se incluyen:

- Si el comportamiento está dirigido a un individuo, a un grupo o a una categoría protegida de personas.
- Si el denunciante es el objeto del abuso o un testigo.
- Si la personas denunciada tiene antecedentes de incumplimiento de las reglas de la plataforma.
- La gravedad del incumplimiento.
- Si el contenido es un tema de legítimo interés público.

En help.twitter.com/forms se pueden encontrar los formularios directos para cualquier tipo de reporte que sobre violaciones a las Reglas de Twitter. También hay opciones directas desde twitter.com y desde la aplicación para reportar Tweets, cuentas, o Mensajes Directos.

Denunciar una cuenta:

1. Abre el perfil que deseas denunciar.
2. Selecciona el ícono de *contenido adicional* .
3. Selecciona *Denunciar a @nombredeusuario* y luego selecciona el tipo de violación que deseas denunciar.
4. Dependiendo de tu selección, la plataforma te pedirá información adicional sobre el problema que estás denunciando.

Denunciar un Tweet:

1. Dirígete al Tweet que quieres denunciar.
2. Pulsa el icono de ***contenido adicional*** situado en la parte superior del Tweet.
3. Selecciona *Denunciar Tweet.*
4. Dependiendo de tu selección, la plataforma te pedirá información adicional sobre el problema que estás denunciando.

Denunciar un Mensaje Directo:

1. Haz clic en la conversación de Mensajes Directos que quieres denunciar.
2. Haz clic en el ícono de ***contenido adicional*** .
3. Selecciona *Denunciar a @nombredeusuario.*
4. Dependiendo de tu selección, la plataforma te pedirá información adicional sobre el problema que estás denunciando.

Avisos en Twitter y su Significado

Tomando en cuenta algunas de las medidas señaladas anteriormente, Twitter coloca un aviso en la cuenta o Tweet para brindar más contexto a las personas sobre las medidas de cumplimiento que se han tomado. Es importante entender el significado de estos anuncios para saber la diferencia entre, por ejemplo, una cuenta que ha sido desactivada por la persona o una cuenta que ha sido suspendida temporalmente; o entre un Tweet que ha sido eliminado por el autor original y un Tweet que ha violado las reglas de la plataforma. Algunos de los avisos que se pueden encontrar en Twitter son:

> Este Tweet puede incluir contenido delicado.

Aviso de contenido multimedia delicado, no apto para menores o que incluye violencia gráfica. En este caso, las personas son informadas que si deciden hacer clic en el aviso, verán contenido multimedia delicado.

> El siguiente elemento multimedia incluye contenido potencialmente delicado. **Cambiar la configuración**

Aviso de contenido de interés público. Esto corresponde a casos muy específicos en los que se determina que un Tweet que incumple las reglas de Twitter es de interés público, por lo que seguirá accesible en la plataforma. Dicho Tweet se coloca detrás de un aviso que explica la excepción y da la opción de ver el Tweet si así lo desea la persona.

> Este Tweet incumplió las Reglas de Twitter relativas a [regla específica]. Sin embargo, Twitter determinó que puede ser de interés público que dicho Tweet permanezca accesible. **Más información**

> Este Tweet incumplió las Reglas de Twitter. **Más información**

Aviso en relación con un Tweet eliminado que incumplió las reglas. Si un Tweet que incumple las reglas todavía no ha sido eliminado por la persona que lo Twitteó, este se oculta detrás de un aviso y la cuenta permanece bloqueada hasta que el autor elimine el Tweet. Una vez eliminado el Tweet, el aviso permanece en la plataforma durante 14 días más.

Aviso en relación con un Tweet de una cuenta suspendida. Tweets de una cuenta suspendida por violaciones a las Reglas de Twitter aparecen ocultos detrás de un aviso con esta información.

> Este Tweet es de una cuenta suspendida. **Más información**

> Denunciaste este Tweet. **Ver**

Aviso en relación a un Tweet denunciado. Al denunciar un Tweet, la cuenta que hace la denuncia verá el Tweet detrás de un aviso que así lo indica y tiene la opción de elegir si desea o no volver a ver dicho contenido.

Aviso en relación a un Tweet de una cuenta bloqueada o silenciada. Si silenciaste o bloqueaste una o varias cuentas y otra persona comparte sus Tweets, el contenido de los mismos aparecerá oculto detrás de un aviso, pero tendrás la opción de hacer clic para verlo.

> Este Tweet es de una cuenta que silenciaste. **Ver**

Si silenciaste palabras o hashtags, recibirás un aviso similar:

> Este Tweet incluye una palabra que silenciaste. **Ver**

El titular de esta cuenta restringe quiénes pueden ver sus Tweets. **Más información**

Aviso en relación a un Tweet con visibilidad limitada. Este aviso aparece en casos en los que un Tweet no está disponible para ver si, por ejemplo:
Es un Tweet de una cuenta protegida, es decir, solo las personas que lo siguen pueden ver su contenido o es un Tweet de una cuenta que te tiene bloqueado/a.

Este Tweet no está disponible. **Más información**

El Tweet fue eliminado por el autor del mismo.

Este Tweet es de una cuenta que ya no existe. **Más información**

El Tweet es de una cuenta que fue desactivada.

Aviso en relación a una cuenta que debe verificar su autenticidad. Cuando se le solicita al titular de una cuenta que verifique su autenticidad con un número de teléfono o una dirección de correo electrónico, dicha cuenta es temporalmente restringida hasta que se proporcione la información requerida.

Precaución: Esta cuenta está temporalmente restringida. **Sí, ver perfil**

Esta cuenta no existe. Intenta hacer otra búsqueda.

Aviso de cuenta desactivada. Los titulares de cuentas tienen la capacidad de desactivar su cuenta en cualquier momento. Cuando el titular de una cuenta la desactiva, la página se muestra como no disponible.

Aviso de suspensión permanente. Si una cuenta ha sido suspendida por violar las Reglas de Twitter, se indica esta información en la cuenta en cuestión.

Twitter suspende las cuentas que incumplen las Reglas de Twitter.

Informe de Transparencia de Twitter

Siguiendo su principio de transparencia y bajo la creencia de que el intercambio libre de información puede tener un impacto positivo, desde el 2012 Twitter ha publicado un informe semestral de transparencia. En este informe se presenta información sobre los requerimientos de información y de eliminación que Twitter recibe de las autoridades, notificaciones de infracción de derechos de autor y de marcas comerciales, aplicación de las Reglas de Twitter, e instancias de manipulación de la plataforma, incluyendo operaciones de información que la plataforma ha determinado que cuentan con el apoyo de Estados.

Controla tu experiencia en Twitter

Twitter es un lugar pensado para compartir ideas e información, conectarse con la comunidad y conocer el entorno en donde se vive. Con el propósito de proteger esta experiencia, Twitter ofrece herramientas que permiten personalizar y controlar dicha experiencia, lo que se ve, y lo se le permite a otros ver de uno mismo, de forma que todas las personas puedan expresarse en Twitter con seguridad.

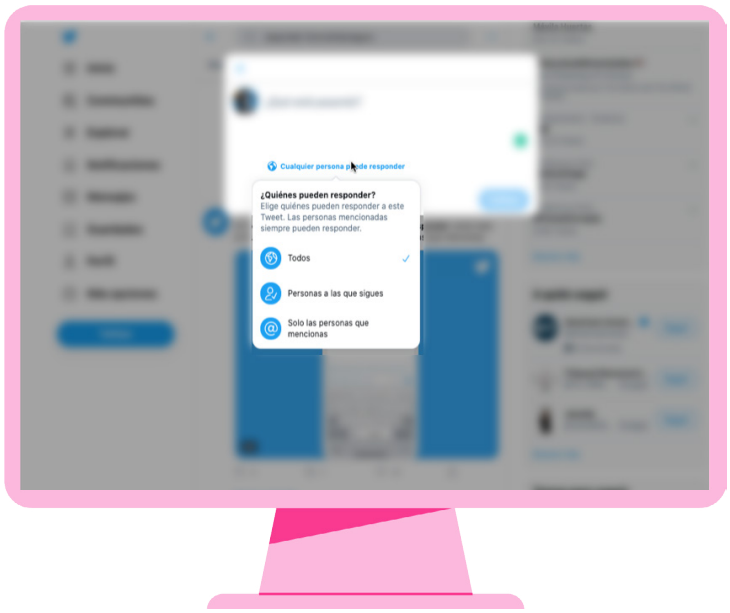
Filtro de Notificaciones

La cronología de Notificaciones muestra las interacciones con otras cuentas de Twitter, como las menciones, los Me gusta, los Retweets y quién ha comenzado a seguirte. Si se reciben respuestas o menciones no deseadas, puedes filtrar los tipos de notificaciones que recibes. En la configuración de las Notificaciones, existen tres opciones para filtrar las notificaciones que se reciben: filtro de calidad, palabras silenciadas y filtros avanzados.

- **Filtro de calidad:** filtra el contenido de menor calidad para que no aparezca en tus notificaciones (por ejemplo, los Tweets duplicados o contenido que parezca automatizado) pero no se filtran las notificaciones de las personas a las que se sigue o de las cuentas con las que se interactuó recientemente.
- **Palabras silenciadas:** silencia las notificaciones que incluyan palabras y frases específicas que no se quieren ver en las notificaciones.
- **Filtros Avanzados:** permiten desactivar las notificaciones de ciertos tipos de cuentas, como por ejemplo, cuentas que no se siguen entre ellas, o que usan la foto de perfil predeterminada de Twitter, o no tienen un correo electrónico o número de teléfono registrado para confirmar su autenticidad.

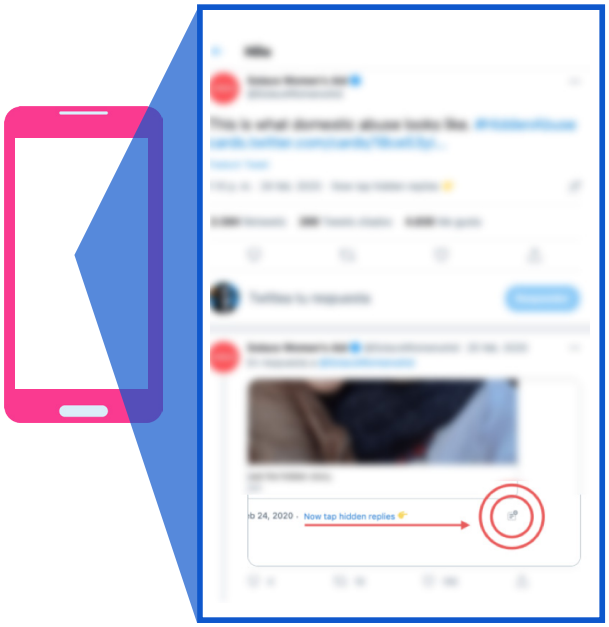
Control de Respuestas

Cuando se escribe un Tweet se puede elegir quién puede responder al mismo. De forma predeterminada, está seleccionada la opción *Cualquier persona puede responder* en la parte inferior izquierda en el compositor del Tweet. Al hacer clic o pulsar dicha opción antes de publicar un Tweet, se puede elegir quiénes pueden responder a ese Tweet en específico. Las opciones son: *Todos, Personas que sigues,* o *Solo las personas que mencionas en ese Tweet.*



Las personas verán si se ha establecido un límite sobre quién puede responder a un Tweet y no se pueden cambiar las restricciones una vez que se haya publicado un Tweet.

Respuestas Ocultas



Para ayudar a las personas a mantener el control de las conversaciones que han iniciado, Twitter tiene una herramienta que le permite al autor del Tweet ocultar respuestas específicas que su contenido recibe. Todas las personas pueden seguir accediendo a las respuestas ocultas a través del ícono ***respuesta oculta*** , que aparece en el Tweet original cuando hay respuestas ocultas. El autor del Tweet puede ocultar o dejar de ocultar una respuesta en cualquier momento y el autor de dicha respuesta no recibirá una notificación al respecto.

Para ocultar una respuesta, pulsa o haz clic en el ícono de ***contenido adicional*** del Tweet que quieres ocultar, selecciona *Ocultar respuesta* y confirma. Para ver las respuestas ocultas, pulsa o haz clic en el ícono ***respuesta oculta*** que estará disponible en la esquina inferior derecha del Tweet inicial.

Silenciar

Se pueden silenciar cuentas, palabras o conversaciones:

Silenciar una cuenta de Twitter significa que los Tweets de esa cuenta no aparecerán en tu cronología de inicio. Las cuentas silenciadas no reciben ningún tipo de aviso para informarles que han sido silenciadas. Además, las notificaciones de menciones de dichas cuentas seguirán activas, así como el intercambio de Mensajes Directos. También se pueden silenciar cuentas que no se siguen para ocultar sus Tweets de la cronología de notificaciones.

Para silenciar una cuenta, pulsa el ícono de ***contenido adicional*** en un Tweet y haz clic en *Silenciar*. Para dejar de silenciar una cuenta, visita el perfil de Twitter de la cuenta silenciada, y haz clic en el ícono de ***contenido adicional de la cuenta*** y luego en *Dejar de silenciar a @nombredeusuario* para dejar de silenciar.

Silenciar palabras, frases, nombres de usuario, emojis o hashtags. La opción de silenciar hará que no aparezcan estos Tweets en la pestaña de Notificaciones, notificaciones push, notificaciones de correo electrónico, cronología de inicio y respuestas, aunque estos Tweets aún serán visibles en resultados de búsquedas. Para agregar o eliminar elementos de tu lista de silenciados:

1. Haz clic en *Configuración y privacidad* en el menú desplegable de tu imagen de perfil.
2. Haz clic en *Preferencias de contenido*.
3. Haz clic en *Silenciado*.
4. Haz clic en *Palabras silenciadas* y luego en *Añadir*.
5. Ingresa la palabra o el hashtag que deseas silenciar, uno a la vez.
6. Selecciona *Cronología* de inicio si deseas silenciar la palabra o la frase en tu Cronología de inicio o *Notificaciones* si deseas silenciar la palabra o la frase en tus Notificaciones.
7. Elige la opción *De cualquier usuario* o *Solo de personas que no sigo*.
8. En la sección *¿Por cuánto tiempo?* elige entre las opciones *Para siempre, 24 horas desde ahora, 7 días desde ahora* o *30 días desde ahora*.
9. Haz clic en *Aceptar*.

Silenciar conversaciones hace que se dejen de recibir las notificaciones de una conversación. Cuando se silencia una conversación, no se recibe ninguna notificación relacionada pero los Tweets de la conversación aún son visibles en la cronología y también al hacer clic en el Tweet original. Para silenciar una conversación:

1. Haz clic en el icono de ***contenido adicional*** de cualquier Tweet o respuesta de la conversación que deseas silenciar.
2. Haz clic o pulsa *Silenciar esta conversación.*
3. Pulsa o haz clic para confirmar.

Bloquear

Al bloquear una cuenta en Twitter, se impide que esa cuenta interactúe con la la cuenta que la ha bloqueado. El bloqueo puede resultar útil para controlar las interacciones no deseadas provenientes de cuentas con las que a la persona no le interesa relacionarse. Las cuentas bloqueadas no pueden ver los Tweets, interacciones, a quién sigue o quién sigue a la cuenta que la la bloqueó siempre y cuando tengan una sesión abierta en Twitter. Tampoco se recibirán notificaciones de cuentas bloqueadas ni se verán sus Tweets en la cronología. Es posible que la persona que maneja una cuenta que ha sido bloqueada note que fue bloqueada si intenta visitar el perfil o seguir a la cuenta que lo/la bloqueó, pero no recibirá notificaciones que les avisen del bloqueo.

Para acceder a esta opción, pulsa el ícono de ***contenido adicional***  en un Tweet de dicha cuenta o desde su perfil y haz clic en *Bloquear*. Para desbloquear una cuenta ve al perfil de la cuenta de Twitter, haz clic en el botón de *Bloqueado* y confirma que deseas desbloquear la cuenta.

CONSIDERACIONES FINALES

El contenido presentado en este documento, desarrollado por la **OEA** y **Twitter**, pretende informar y concientizar a las personas sobre el manejo, consumo y distribución de información en línea, con un enfoque en las redes sociales, particularmente en Twitter. Esta guía tiene el propósito de contribuir a que todas las personas, incluyendo periodistas, autoridades gubernamentales y organizaciones, logren una mejor comprensión sobre la importancia de la alfabetización y seguridad cibernética.

El incremento de las actividades digitales ha evidenciado vulnerabilidades preexistentes del espacio digital. El crecimiento en el número de ataques cibernéticos y la digitalización de innumerables procesos cotidianos reafirman la necesidad de aumentar la alfabetización y concientización de buenas prácticas de ciberseguridad. Esta edición de la guía brinda una visión renovada sobre herramientas y buenas prácticas para consumir información y contenido de manera segura y responsable.

Las plataformas tecnológicas y las redes sociales han creado nuevas modalidades de comunicación, ampliando las posibilidades de participación política al permitir que el entorno digital esté involucrado en los procesos democráticos. La alfabetización digital es esencial para el fortalecimiento de la democracia, dado que es un instrumento que contribuye a una participación masiva que facilita una participación ciudadana activa y responsable. De igual manera, la alfabetización contrarresta fenómenos como la desinformación, la injerencia de actores externos en política interna, entre otros elementos, que directa o indirectamente impactan e influyen en los procesos democráticos.

A través de las diferentes secciones, se ha recopilado información relacionada con la ciberseguridad y el autocuidado digital, la cual ha sido actualizada para presentar las nuevas amenazas y herramientas surgidas a raíz de los cambios en el entorno y el aumento del teletrabajo. Asimismo, la guía incluye recomendaciones específicas en relación al consumo de información de Twitter y la actualización de sus reglas de uso, y herramientas fundamentales para la experiencia de las personas en la plataforma.

DADO QUE LA ALFABETIZACIÓN Y SEGURIDAD DIGITAL, ASÍ COMO LA COMPLEJIDAD DE LOS DELITOS EN LÍNEA, TIENEN UNA NATURALEZA DE CONSTANTE DESARROLLO, ES VITAL PERMANECER INFORMADOS Y ACTUALIZADOS EN TORNO A LOS PRODUCTOS Y POLÍTICAS QUE AFECTAN EL DESENVOLVIMIENTO E INTERACCIONES EN MEDIOS DIGITALES Y REDES SOCIALES.

El uso intensivo de las tecnologías digitales en el mundo permanecerá en la vida cotidiana, por lo que la ciberseguridad y la alfabetización, aplicadas por parte de cada individuo, son sumamente importantes para garantizar capitalizar el beneficio de la conectividad y disponibilidad de información de manera segura, a fin de brindar un entorno de mayores posibilidades de desarrollo, así como de bienestar social y fortalecimiento de la democracia.

Referencias

BBC News Mundo. (2020). *Coronavirus: la advertencia de la OMS sobre los estafadores que están usando el nombre de la organización para robar dinero y datos.* https://www.bbc.com/mundo/noticias-52009138

Duclkin, Paul. (2020). *Dirty little secret extortion email threatens to give your family coronavirus. Sophos* https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/

Eset. *Social Engineering (in cybersecurity).* https://www.eset.com/int/social-engineering-business/

Forbes, Jac. (2019). Guía de seguridad periodística para elecciones. Comité de Protección de Periodistas. https://cpj.org/es/2019/10/guia-de-seguridad-periodistica-para-elecciones/#harassed

Germain, Thomas. (2019). *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.* Consumer Reports. https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

INCIBE y OSI. (2020). *Detectada oleada de falsos correos de sextorsión o infección de COVID19.* https://www.osi.es/es/actualidad/avisos/2020/04/detectada-oleada-de-falsos-correos-de-sextorsion-o-infeccion-de-covid19

Marsh y Microsoft. (2020). *Estado de Riesgo Cibernético en Latinoamérica en Tiempo del COVID-19.* https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

Media and Information Literacy for the Sustainable Development Goals. Grizzle, A and Singh, J. (2016). In the MILID Yearbook 2016.

News and Media Literacy: What is Media Literacy, Common Sense Media: https://www.commonsensemedia.org/news-and-media-literacy/what-is-digital-literacy (consultado el 18 de agosto de 2019).

NortonLifeLock. *¿Qué es la ingeniería social?*. https://lam.norton.com/Internetsecurity-emerging-threats-what-is-social-engineering.html

Organización Mundial de la Salud. (2020). *WHO reports a fivefold increase in cyber attacks, urges vigilance.* https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Organización de las Naciones Unidas Comisión Económica para América Latina y el Caribe. Informe Especial COVID-19 (2020). *Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.* https://repositorio.cepal.org/bitstream/handle/11362/45938/4/S2000550_es.pdf

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2016). *Alfabetización.* https://es.unesco.org/themes/alfabetizacion

Organización de los Estados Americanos y Twitter. (2019). *Alfabetismo y Seguridad Digital: Mejores Prácticas en el Uso de Twitter.* https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf

Organización de los Estados Americanos. (2019). *Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales.* http://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf

Porter, Taryn. (2020). COVID-19 *Scam Alters. Cybercrime Support Network.* https://cybercrimesupport.org/covid-19-scam-alerts/

Roesler, Martin.(2020). *Working From Home? Here's What You Need for a Secure Setup.* Trend Micro. https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup

Software Lab.org. *¿Qué es la ingeniería social?: La definición y los 5 ejemplos principales Qué es ingeniería social.*https://softwarelab.org/es/que-es-ingenieria-social/

Stone, Jeff. (2020). *How scammers use fake news articles to promote coronavirus 'cures' that only defraud victims.* Cyberscoop. https://www.cyberscoop.com/coronavirus-cure-scam-social-media-riskiq/

Trend Micro.(2020). *Developing Story: COVID-19 Used in Malicious Campaigns.* https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

U.S. Department of Homeland Security. (2019). *Social Media Plan Guide: Science and Technology Directorate.* https://www.dhs.gov/sites/default/files/publications/social_media_plan_guide_09_20_2019.pdf

We Live Security y eset. (2020). *Informe de Amenazas. Segundo Trimestre de 2020.* https://www.welivesecurity.com/wp-content/uploads/2020/08/Q2-2020_Threat_Report-ESP.pdf

ALFABETIZACIÓN Y SEGURIDAD DIGITAL:

LA IMPORTANCIA DE MANTENERSE SEGURO E INFORMADO

OEA | Más derechos para más gente