Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Diecisiete

Julio: Protección en Redes Sociales "Privacidad en línea”

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Diecisiete
Julio de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Diego Fernando Medina Soto
Director CCAV Facatativá

Estado legal:
Periodicidad: Quincenal
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 17

Julio 2023

Protección en redes sociales "Privacidad en línea"

Autores:

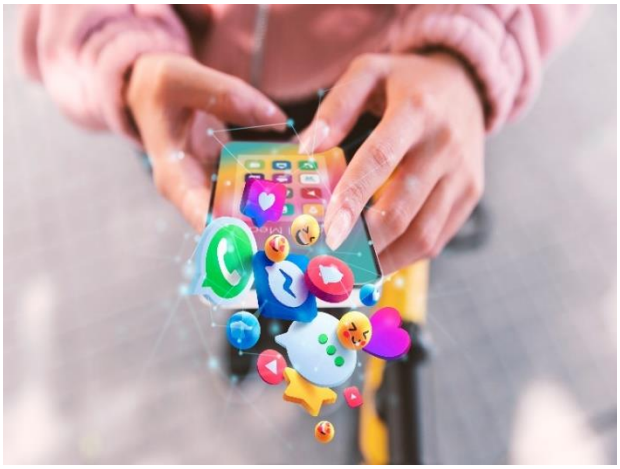
Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Yenny Stella Nuñez Álvarez
CSIRT Académico UNAD
https://orcid.org/0000-0002-6868-6278

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción



Fuente: https://www.freepik.es/foto-gratis/manos-sosteniendo-concepto-redes-sociales-telefonos-inteligentes_38689780.htm#query=redes%20sociales&position=0&from_view=search&track=ais

El imparable ascenso de las redes sociales a nivel global es evidente. Se han transformado en las herramientas de publicidad y difusión de contenidos más destacadas y eficaces en un mundo cada vez más inmerso en lo digital. Sin embargo, en este panorama surge una preocupación evidente: la privacidad, la protección de los datos y la correcta administración de la información especialmente en redes sociales como: Facebook, Twitter, Instagram, LinkedIn, TikTok. Lamentablemente, algunos usuarios no consideran relevante configurar adecuadamente estas plataformas, que dentro de sus políticas ofrecen opciones para activar restricciones, limitar accesos y establecer ciertos niveles de aseguramiento.

Otra situación presentada es que los usuarios de las redes sociales a menudo incurren en el error de compartir una cantidad excesiva de información, lo cual puede ser aprovechado por ciberdelincuentes mediante la recopilación de datos, los cuales pueden ser utilizados para construir perfiles sólidos con el objetivo de llevar a cabo ataques, suplantación de identidad, engaños o estafas de manera más efectiva.

Desarrollo

Privacidad en redes sociales: Cómo configurar y gestionar adecuadamente la privacidad de los perfiles en las principales redes sociales.

No se puede desconocer que las redes sociales desempeñan un papel fundamental al conectar a las personas con el mundo que les rodea. Estas plataformas permiten interacciones entre individuos que comparten intereses afines, ofrecen acceso a una amplia gama de información sobre emprendimientos, productos y servicios de diversas organizaciones, y brindan la oportunidad de expresar opiniones y mostrar creaciones personales. Además, las redes sociales se han convertido en fuentes de entretenimiento variado y en ventanas a una amplia gama de publicaciones en áreas tan diversas como empleo, noticias, educación, aspectos sociales y laborales, así como entretenimiento y ocio. Sin embargo, en medio de estas ventajas, no todo es color de rosa, estas plataformas están expuestas a riesgos cibernéticos, que van desde la propagación de virus a través de mensajes masivos hasta la extorsión y el ciberterrorismo.

Fuente: https://www.freepik.es/foto-gratis/mujer-hombre-tiro-medio-casa_13161029.htm?query=cyber#from_view=detail_alsolike

El phishing también presenta una amenaza considerable, representado por cuentas y perfiles falsos diseñados para engañar, robar, estafar o recopilar información confidencial. Además, el ciberacoso emerge como un problema preocupante, en el cual personas malintencionadas hostigan a otros mediante la amenaza o intimidación a través de fotos, videos, mensajes o información invasiva, comprometiendo la tranquilidad y el bienestar de los usuarios de estas plataformas sociales. En este contexto, se requiere que se apliquen buenas prácticas en la gestión y publicación de contenidos y se implemente una configuración correcta de la privacidad y seguridad de las cuentas de usuario en este tipo de plataformas de interacción social.

Configurar y gestionar la privacidad de los perfiles en las principales redes sociales

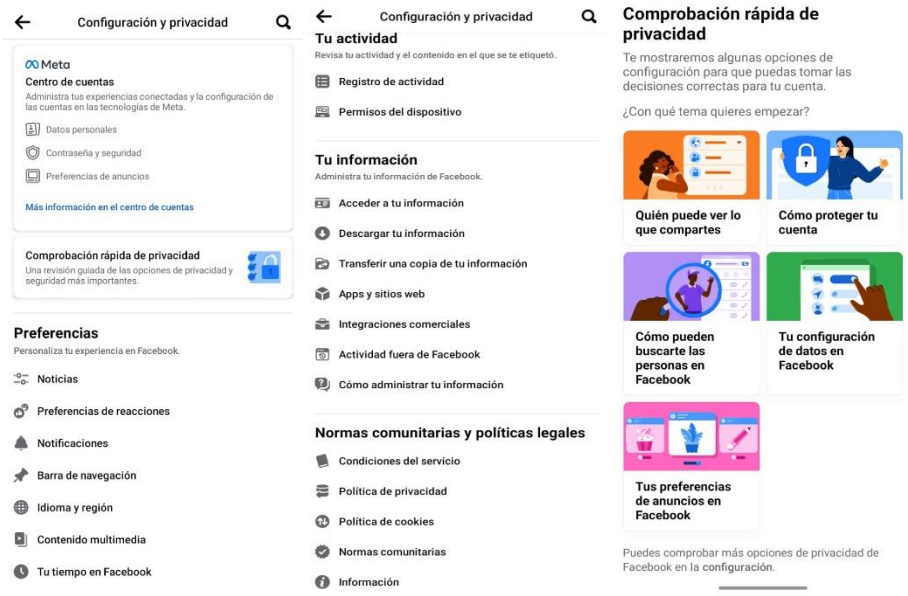
Cuando se crea o utiliza un perfil en una red social, es altamente recomendable llevar a cabo una configuración precisa tanto en términos de privacidad como de acceso a la información que se comparte. Esto implica definir cuidadosamente qué individuos tendrán la posibilidad de acceder a dicho contenido. A continuación, se detallan las sugerencias y pasos necesarios para gestionar de manera efectiva la seguridad y privacidad en algunas de las redes sociales más usadas a nivel global:

Facebook:

En la esquina superior derecha en **Configuración y privacidad > Comprobación rápida y privacidad** o en **Configuración y privacidad>preferencias**.

Facebook ofrece como se observa en la ilustración 1, opciones de administración de cuenta, proporcionando al usuario varias secciones para personalizar la privacidad, desde quien puede ver lo que se comparte, protección de la cuenta, cómo pueden buscarnos las personas en Facebook, la configuración de nuestros datos en Facebook, control de etiquetado de fotos e historias, nuestras preferencias de anuncios en Facebook. Sólo es seguir los pasos en cada opción y decidir cuál es el nivel de privacidad que va a configurarse el perfil[1].

Ilustración 1 configuración privacidad Facebook



Fuente. CSIRT Académico UNAD

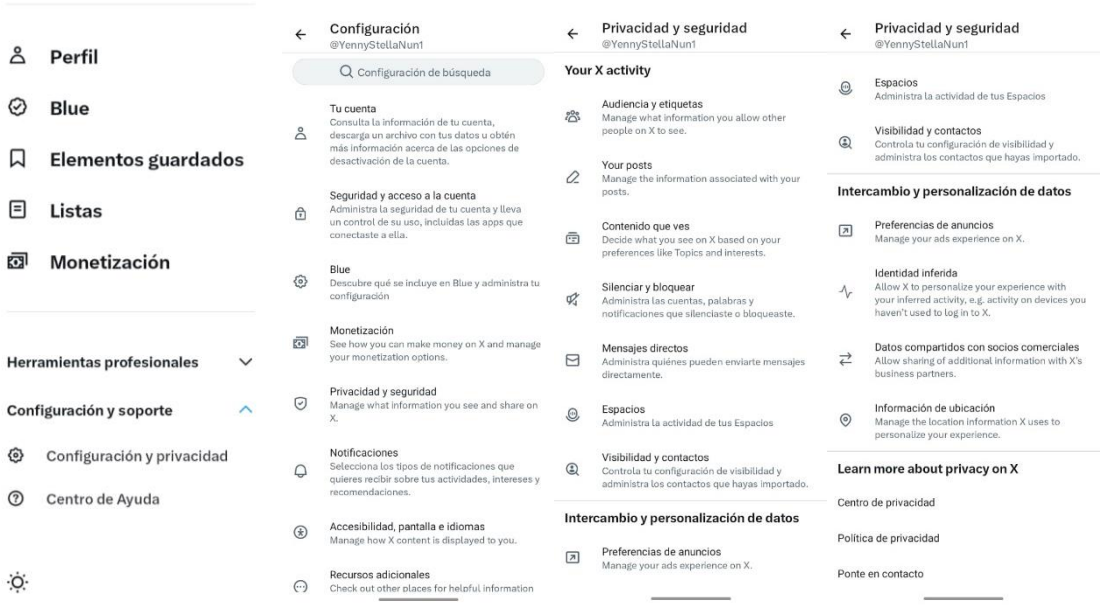
Twitter o actualmente X:

Para la Configuración de privacidad y seguridad de twitter o X es necesario realizar clic en la foto de perfil y ubicar la opción de **Configuración y soporte**. Posteriormente localizar la pestaña **Privacidad y seguridad.** Una vez dentro de esta opción se puede iniciar con la configuración de los mensajes en X, anteriormente conocidos como tweets, tienen la capacidad de recibir una capa adicional de protección al configurarse de manera específica[2]. Esta configuración permite que únicamente aquellos seguidores se aprueben tengan la capacidad de visualizar los mensajes o publicaciones compartidas en la plataforma. Además, se tiene el control total sobre quiénes tienen la autorización para responder a los mensajes o post que se comparten en los perfiles. Adicionalmente, se puede gestionar quiénes tienen el privilegio de seguirnos, dándonos la posibilidad de bloquear a aquellas cuentas no deseadas o con las que no deseamos interactuar. Podemos restringir la

[1] Modificar tu configuración de privacidad de Facebook | Servicio de ayuda de Facebook
[2] Cómo proteger y desproteger tus Tweets | Ayuda de Twitter

capacidad de que nos etiqueten o mencionen en publicaciones, otorgándonos un mayor control sobre nuestra visibilidad o presencia en la plataforma. Entre otras opciones como se pueden ver en la ilustración 2 las cuales se pueden personalizarse de acuerdo a las preferencias y al nivel de privacidad que se desee establecer.

Ilustración 2 configuración privacidad Twitter o X



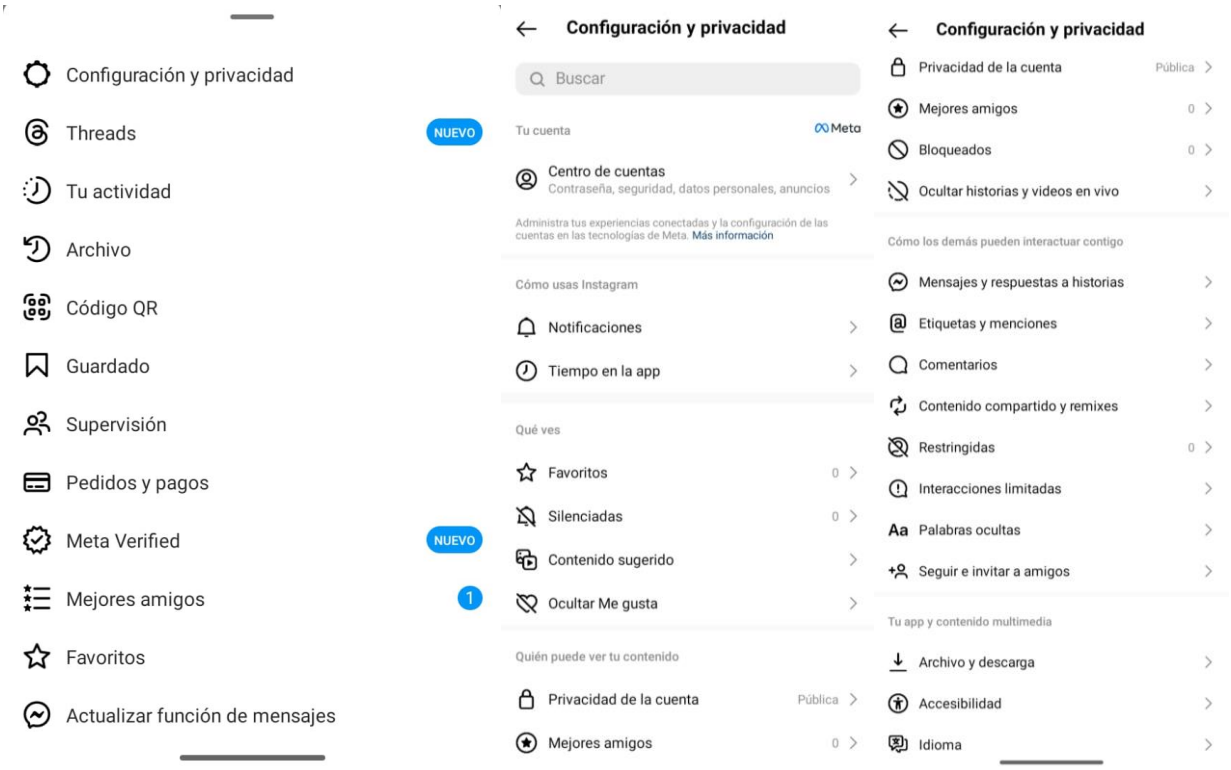
Fuente. CSIRT Académico UNAD

Instagram:

En la esquina superior derecha dentro del perfil de Instagram, se puede acceder a la sección de **Configuración > Privacidad**. Aquí, se tiene la posibilidad de mejorar la privacidad de forma personalizada[3]. Se puede empezar activando la opción de **Cuenta privada,** lo que nos permite decidir quiénes tienen acceso a nuestras fotos y videos. Además, en esta sección, se facilita el control total sobre los comentarios de nuestras publicaciones. Igualmente, se tiene la opción de habilitar un filtro y bloqueo de palabras clave u oraciones que puedan contener expresiones de odio o estar relacionadas con el ciberacoso, asegurando que el ambiente sea respetuoso. Asimismo, se puede gestionar el etiquetado de las fotos en las que hemos sido etiquetados de manera manual antes de que aparezcan en nuestro perfil de Instagram. Esto brinda un mayor control sobre las imágenes que están vinculadas al perfil. La plataforma también ofrece herramientas para la administración de contraseñas, preferencias de inicio de sesión y métodos de recuperación. Estas opciones adicionales de configuración nos permiten fortalecer aún más la seguridad de la cuenta y proteger los contenidos multimedia. Para obtener una visión más completa de todas estas opciones de privacidad y configuración, se puede observar la ilustración 3 las diversas opciones de configuración de privacidad y seguridad de esta plataforma.

[3] Seguridad y privacidad de Instagram | Información sobre Instagram

Ilustración 3 configuración privacidad Instagram



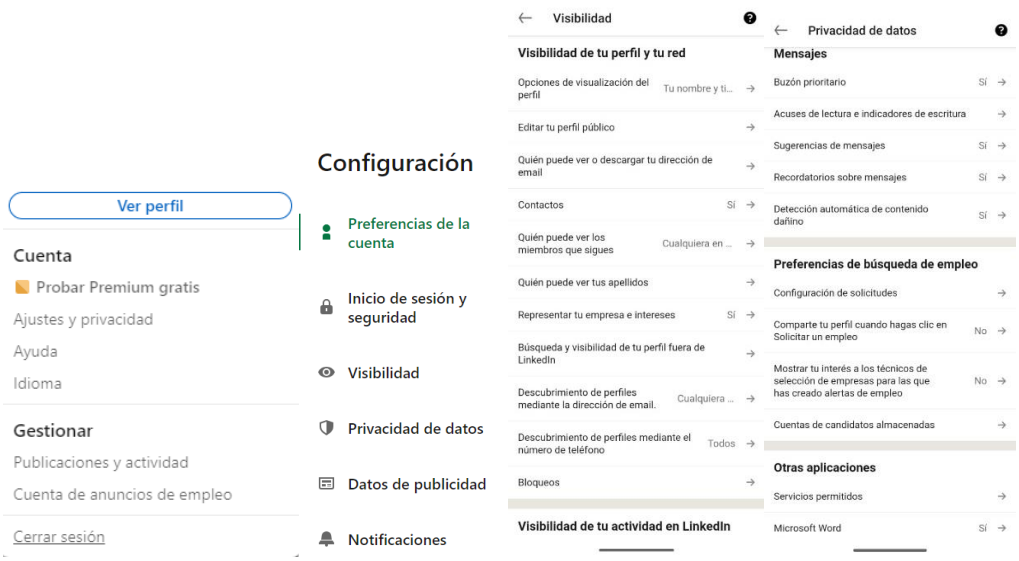
Fuente. CSIRT Académico UNAD

LinkedIn:

En el caso de linkedIn la opción de Configuración de privacidad y visibilidad se ubica realizando un clic sobre la imagen de perfil seleccionando **Configuración >ajustes y privacidad>Visibilidad**, se tiene se puede establecer si se quiere compartir las actualizaciones de la actividad den la red con nuestros contactos o simplemente reservarlas de forma privada[4]. **Configuración>ajustes y privacidad>Privacidad de los datos**, se puede habilitar o deshabilitar qué información se muestra en el perfil según los intereses o preferencias. Las características de este tipo de configuración se puede observar en la ilustración 4 a continuación:

[4] Cómo administrar la configuración de privacidad en LinkedIn

Ilustración 4 configuración privacidad LinkedIn



Fuente. CSIRT Académico UNAD

Riesgos de la divulgación de información personal: Los peligros asociados con la revelación excesiva de información personal en las redes sociales y cómo minimizarlos.

Además de emplear las herramientas de configuración de seguridad y privacidad proporcionados por las diversas redes sociales para resguardar la información y los datos que se difunden públicamente diariamente, resulta crucial mantener una conciencia sobre la cantidad de contenido que se comparte. Especialmente, es importante evitar la exposición excesiva de información personal en línea, ya que inadvertidamente se podría entregar datos sensibles que los ciberdelincuentes podrían aprovechar con múltiples propósitos.

La sobreexposición de información se ha convertido en una realidad que todos reconocemos, especialmente en una sociedad saturada por una variedad de dispositivos móviles que simplifican la publicación instantánea de fotos, videos o transmisiones en vivo de innumerables eventos por parte de cualquier individuo, a menudo sin ningún tipo de filtro. Asimismo, se ha observado una tendencia creciente en la incursión de roles como youtubers, influencers, tiktokers, creadores de contenido en plataformas como las redes sociales que en ocasiones dejan al descubierto información personal de ellos y de otras personas.

Muchas veces en el afán de conseguir popularidad o de obtener muchos seguidores en redes sociales, no se pone limite a la información y datos que se publica, aun sabiendo que existen riesgos informáticos como robo de identidad, ingeniería social, suplantación de identidad, ciberacoso, ataques dirigidos, violación de la privacidad, exposición a malware entre otros, como se describe en la ilustración 5.

Ilustración 5 Riesgos informáticos en las redes sociales

Fuente : https://www.freepik.es/vector-gratis/seguridad-datos-global-seguridad-datos-personales-ilustracion-concepto-linea-seguridad-datos-ciberneticos-seguridad-internet-o-privacidad-proteccion-informacion_12953623.htm#query=ataques%20informaticos&position=2&from_view=search&track=ais

La realidad digital nos expone a diferentes ataques cibernéticos, intrusiones o perdidas de información sino tomamos en serio las alertas o peligros palpables en la red. Para mitigar estos riesgos; es esencial practicar una gestión cuidadosa de la información compartida en línea. Esto implica limitar la cantidad de detalles personales publicados, ajustar adecuadamente las configuraciones de privacidad en las redes sociales, ser cauteloso al aceptar solicitudes de amistad o conexiones de personas desconocidas y ser consciente de las posibles consecuencias antes de publicar cualquier contenido en línea.

Boletín de Ciberseguridad

Protección contra el robo de identidad: Cómo prevenir y detectar intentos de suplantación de identidad en las redes sociales.

El robo de identidad se produce cuando una persona de forma ilícita hace uso de los datos personales o financieros de otra persona sin su consentimiento para realizar diferentes fraudes con tarjetas de crédito, obtener préstamos, adquirir productos y servicios, cometer delitos, entre otros. Para prevenir este tipo de ataque se requiere de buenas prácticas como:

- **Asegurar la privacidad y la seguridad de tus perfiles** en diversas plataformas digitales y redes sociales mediante una configuración cuidadosa y adecuada.
- **Fortalecer las contraseñas** en cada plataforma empleando combinaciones sólidas de caracteres, números y símbolos para dificultar su suposición. Evita la inclusión de información personal como fechas de nacimiento o nombres de familiares. Asegura una capa adicional de protección al optar por contraseñas distintas para cada servicio.
- **Optimizar la seguridad de los diferentes perfiles activando la autenticación de dos factores (2FA).** Esta medida añade un nivel adicional de protección al requerir una verificación extra, como un código enviado al teléfono o correo electrónico, además de la contraseña.
- **Aplicar filtro a las solicitudes de amistad o conexiones que recibas.** No es necesario aceptar todas las invitaciones; hay que asegurarse de conocer a la persona o usuario que busca unirse a la red. Manteniendo la cautela al verificar la autenticidad y confiabilidad de la información y perfiles del posible contacto, evitando aceptar sin previa confirmación.
- **Evitar la publicación de información personal** como por ejemplo número de teléfono, fechas de nacimiento, direcciones, ubicación real, entre otros.
- **Monitorear los perfiles** regularmente para verificar si existe algo fuera de lo común como actividades sospechosas, irregularidades en la lista de contactos o amigos, cambios de configuración de la privacidad, conexiones desconocidas, etc.
- **Permanecer alerta ante mensajes sospechosos o inusuales** que ofrezcan promociones excepcionales, oportunidades laborales sorprendentes o premios inesperados. Estos mensajes podrían esconder intentos de engaño, estafas o enlaces maliciosos diseñados para obtener acceso a tus datos personales o financieros
- **Realizar investigaciones por tu cuenta** buscando perfiles similares en varias plataformas. Este esfuerzo contribuye a identificar posibles suplantaciones de identidad o perfiles fraudulentos que podrían estar utilizando nuestra información de manera indebida. Si es el caso hay que denunciarlas.
- **Instalar actualizaciones,** para reducir al mínimo los riesgos de ataques informáticos, es esencial mantener los dispositivos y software al día mediante la instalación regular de las últimas versiones de seguridad disponibles.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

Correo: csirt@unad.edu.co

Twitter: @csirtunad

Página web: https://csirt.unad.edu.co