Pontificia Universidad
JAVERIANA
Colombia

Protocolo para la prevención y atención de incidentes de seguridad en redes sociales

PROTOCOLO PARA LA PREVENCIÓN Y ATENCIÓN DE INCIDENTES DE SEGURIDAD EN REDES SOCIALES

Autores

Pedro Pablo Mejía Salazar – Dirección de Comunicaciones
María Camila Medina Posada – Dirección de Comunicaciones
Paola Andrea Moreno López - Dirección de Comunicaciones
Pedro Alexander Rivera López – Dirección de Tecnologías de Información

Colaboradores

Adriana Díaz Hernández – Dirección de Comunicaciones
Hugo Santiago Caro Jiménez – Dirección de Comunicaciones
Juan Camilo Ramírez Motta – Dirección de Comunicaciones
Nelson Gómez De la Peña – Dirección de Tecnologías de Información
Juan David Acosta Velasco – Dirección de Mercadeo de Programas Académicos
Stephanie Ramírez Moreno - Dirección de Mercadeo de Programas Académicos
Diana Carolina Laverde Escobar – Oficina de Comunicaciones Javeriana Cali

Alexander Marroquín – Edición gráfica y diseño

Bogotá, [28 de febrero de 2022]
Actualizado [14 de junio de 2024]

PROTOCOLO PARA LA PREVENCIÓN Y ATENCIÓN DE INCIDENTES DE SEGURIDAD EN REDES SOCIALES

Contenido

- Filtro de contenido
- Controles de seguridad automáticos

Capítulo III: X

- Restablecer contraseña
- Autenticación de dos factores
- Códigos de respaldo
- Pérdida o cambio de celular
- Aplicaciones y sesiones
- Controles de seguridad automáticos

Capítulo IV: Instagram

- Ajustes de seguridad
- Recuperar contraseña
- Autenticación de dos factores
- Código de respaldo
- Sesiones iniciadas
- Correos electrónicos de Instagram
- Aplicaciones de terceros
- Filtro de contenido
- Controles de seguridad automáticos

Capítulo V: YouTube

- Ajustes de seguridad
- Reestablecer contraseña
- Verificación en dos pasos
- Aplicaciones de terceros
- Controles de seguridad automáticos

Capítulo VI: LinkedIn

- Ajustes de seguridad
- Autenticación de dos factores
- Roles de página
- Controles de seguridad automáticos

Capítulo VII: TikTok

- Ajustes de seguridad
- Restablecer contraseña
- Autenticación de dos factores
- Sesiones iniciadas
- Aplicaciones de terceros
- Filtro de contenido
- Controles de seguridad automáticos

Capítulo VIII: Spotify

- Restablecer contraseña
- Aplicaciones de terceros

Capítulo IX: Gestión de incidentes

- ¿Qué se considera un incidente?
- Categorización de incidentes
- Proceso para la atención de incidentes
- Flujograma de actividades

Glosario

Presentación

Presentación

Objetivo General

Unificar las pautas para que los gestores de redes sociales de la Pontificia Universidad Javeriana eviten y prevengan incidentes de seguridad en las cuentas institucionales y actúen adecuadamente y con prontitud en caso de presentarse situaciones que puedan afectar la reputación institucional o generar pérdida de información.

Objetivos Específicos

- Dar a conocer las recomendaciones y buenas prácticas que se deben aplicar sobre el manejo de los dispositivos (equipos móviles y de cómputo) y aplicaciones con las que se gestionan las redes sociales institucionales y las sugerencias para manejar las contraseñas y permisos de acceso a las cuentas.

- Explicar las configuraciones de seguridad de las redes sociales Facebook, X, Instagram, YouTube, LinkedIn, TikTok y Spotify para que se apliquen en las cuentas de la Universidad Javeriana, para minimicen las posibilidades de incidentes que puedan afectar su gestión.

- Detectar, reportar, controlar, monitorear y responder de manera oportuna y apropiada ante la ocurrencia de un incidente de seguridad presentado en las redes sociales institucionales, estableciendo un proceso para solucionarlos y generando lecciones aprendidas que prevengan la repetición de casos.

Alcance

Este Protocolo pretende ser una guía de uso permanente para que los gestores de redes sociales de la Pontificia Universidad Javeriana prevengan y eviten incidentes de seguridad en las cuentas institucionales, aplicando los lineamientos definidos en este documento por la Dirección de Comunicaciones (DirCom) y la Dirección de Tecnologías de la Información (DTI). Así mismo, establece un proceso para el manejo y la escalada de los incidentes para la oportuna reacción y solución, cuando se puedan atender desde la comunicación o la seguridad informática. Cuando los incidentes requieran de acciones y respuestas de tipo judicial se escalará a las respectivas autoridades de la Universidad.

Actores a los que está dirigido

Este Protocolo está dirigido a las personas que tienen relación directa e indirecta con la gestión de redes sociales institucionales. En primera instancia las unidades encargadas de socializar, presentar y velar por el cumplimiento de este documento son la Dirección de Comunicaciones y la DTI. Los gestores de comunicación de todas las unidades de la Universidad son los principales actores encargados de atender los lineamientos, extensivos también a las empresas que estos contraten para labores relacionadas con las cuentas de redes sociales institucionales.

Responsables y responsabilidades

Comité de Crisis

- Dar lineamientos oportunos para atender y solucionar incidentes que impliquen temas legales o una posible crisis de reputación para la Universidad.

Dirección de Comunicaciones

- Socializar con los gestores de comunicación de la Universidad el contenido del Protocolo y sus actualizaciones.
- Revisar el documento cada 6 meses considerando las actualizaciones de cada red social en sus configuraciones de seguridad, para incluir en el Protocolo las novedades que se encuentren.
- Aplicar todas las recomendaciones del Protocolo en las redes principales de la Universidad: @Unijaveriana.
- Cuando se requiera la contratación de terceros para temas relacionados con la gestión de redes sociales, exigir dentro del contrato el cumplimiento estricto de este Protocolo.
- Ser el primer canal de atención cuando se presente un incidente que reporte alguna de las unidades de la Universidad, para categorizar el incidente y definir si se puede solucionar desde la comunicación o desde las configuraciones que ofrece cada red social.
- Escalar al Equipo de Seguridad Informática de la DTI aquellos incidentes que para su solución requieran atención de personal con conocimientos técnicos en sistemas.
- Aplicar las correcciones y controles de riesgo que se definan en el reporte final cuando se solucione un incidente.
- Informar al Comité de Crisis de la Universidad cuando se detecte un incidente que pueda afectar la reputación institucional o que tenga implicaciones legales.

DTI Equipo de seguridad informática

- Recomendar la implementación de buenas prácticas, políticas, normas, directrices y procedimientos de seguridad para las redes sociales de la Universidad.

- Acompañar el proceso de respuesta a incidentes en redes sociales, teniendo en cuenta que la seguridad de estas se basa en una correcta configuración y administración.
- Atender oportunamente las solicitudes que escale la Dirección de Comunicaciones cuando los incidentes requieran personal con conocimientos técnicos en sistemas.
- Escalar a la Dirección de Comunicaciones los reportes de incidentes que reciban directamente e informar cuando se enteren de un riesgo de *hackeo* o ataque a las redes sociales.
- Trabajar periódicamente con la Dirección de Comunicación en el desarrollo y mejora continua de las configuraciones y parametrizaciones previas.
- Comunicar las vulnerabilidades que se presenten sobre las diferentes redes sociales para proponer oportunidades de mejora a nivel de seguridad de la información.
- Revisar el documento cada 6 meses considerando las actualizaciones de cada red social en sus configuraciones de seguridad, para incluir en el Protocolo las novedades que se encuentren.

GESTORES DE COMUNICACIONES DE LAS UNIDADES

- Aplicar todas las recomendaciones del Protocolo en las redes oficiales de sus respectivas unidades.
- Socializar y vigilar el cumplimiento del contenido del Protocolo y sus actualizaciones con las empresas o personas que la unidad contrate (empleados de planta, contratistas, practicantes, agencias...) para gestionar redes sociales.
- Cuando se requiera la contratación de terceros para temas relacionados con la gestión de redes sociales, exigir dentro del contrato el cumplimiento estricto de este Protocolo.
- Reportar oportunamente a la Dirección de Comunicaciones, a través de ComunicarT (http://intranet.javeriana.edu.co/comunicar-t), los incidentes que detecten en sus redes sociales y participar activamente de la solución, acompañando todo el proceso y facilitando toda la información que se requiera para ello.
- Aplicar las correcciones y controles de riesgo que se definan en el reporte final cuando se solucione un incidente.

TERCEROS CONTRATADOS PARA LA GESTIÓN DE REDES SOCIALES

- Cumplir estrictamente con todas las recomendaciones contempladas en este Protocolo de seguridad.
- Reportar a la unidad que los contrató, oportunamente, los incidentes que detecten en las redes sociales que están gestionando y participar activamente de la solución acompañando todo el proceso y facilitando toda la información que se requiera para ello.

1 Recomendaciones generales

Capítulo I: Recomendaciones Generales

Inicio de sesión

Asegúrese siempre de estar en el dominio oficial de cada red social antes de ingresar las credenciales de inicio de sesión.

- Facebook: www.facebook.com
- X: www.x.com
- Instagram: www.instagram.com
- LinkedIn: www.linkedin.com
- YouTube: www.youtube.com
- TikTok: www.tiktok.com
- Spotify: www.spotify.com

Nunca acceda a las redes institucionales o a sus correos asociados desde un equipo de cómputo de uso público.

Permisos de acceso

Se recomienda que cada unidad otorgue la menor cantidad posible de permisos de administración sobre las cuentas gestionadas (máximo 3 personas). Preferiblemente que sean empleados de planta, no practicantes.

Registro de personas autorizadas

Se recomienda tener una base de datos que contenga toda la información de las personas autorizadas para acceder a las redes sociales institucionales. Estos datos deben ser: nombre, información de contacto (correo electrónico y celular), marca de los equipos desde donde se gestionan las redes y su respectiva dirección IP.

- Para conocer la dirección IP de su equipo puede consultarla en: https://www.cual-es-mi-ip.net/

Equipos corporativos

Se sugiere que la gestión de las redes sociales se haga desde computadores y/o celulares corporativos[1], de uso exclusivo para esta función y evitando que otras personas los usen.

[1] La solicitud para la adquisición de equipos corporativos debe hacerse a la DTI y debe tener un concepto previo de la Dirección de Comunicaciones.

Si se gestiona desde equipos personales, tener en cuenta las siguientes recomendaciones:

- Tener precaución de no abrir al mismo tiempo la cuenta personal y la institucional.
- Si va a publicar, dar me gusta o seguir a un usuario desde su cuenta personal, verifique previamente que no esté en la cuenta institucional.
- Cada vez que descargue una aplicación nueva en el celular, revisar en los términos y condiciones que previamente no esté autorizando acceso a una red social.
- Tener bloqueos de acceso en el celular y en las redes sociales.
- No anotar las contraseñas en el celular.
- Mantener cerrada la sesión de las cuentas institucionales cuando no las esté usando.
- Si es posible, separe horarios para uso de la cuenta personal y para el uso de las cuentas institucionales. De esa manera se evita el riesgo de publicar algo personal en la cuenta institucional.

Protección de acceso a los dispositivos

Los equipos deben contar con medidas de autenticación del usuario. El bloqueo de pantalla con contraseña o las autenticaciones biométricas dificulta el acceso al dispositivo y sus datos.

Redes de *wi-fi*

Las conexiones a las redes de *wi-fi* públicas pueden suponer un riesgo para la seguridad en los equipos asociados a las redes sociales, ya que son fácilmente *hackeadas* a través de ataques con intermediarios (*Man-in-the-Middle*). Una buena forma de evitarlo es apagando la función de conexión automática. También se aconseja contar con una VPN (red privada virtual o *virtual private network*).

Correos y celulares asociados

Las redes sociales deben estar asociadas a correos institucionales y, de ser posible, a números de celulares corporativos. En el caso de YouTube la cuenta se crea desde *Gmail*, pero se sugiere utilizar un correo institucional como respaldo. Los correos y celulares que se utilicen para la gestión de las redes sociales no deben quedar visibles en la descripción del perfil.

Contraseñas

Establecimiento de contraseñas:

- Debe tener mayúsculas, minúsculas, números y signos.
- Se recomienda usar frases de fácil recordación de por lo menos 10 caracteres, cuanto más larga mejor. Puede sustituir números por

letras que se parezcan entre sí (por ejemplo, reemplazar "0" por "o" o "3" por "E").

- También pueden utilizarse frases, fragmentos de canciones o citas importantes, y convertirlas en una contraseña compleja utilizando alguna letra de cada palabra.
- No utilice información personal en su contraseña, como números de teléfono, cumpleaños, el nombre de la institución, etc.
- Utilice contraseñas diferentes a las de sus cuentas personales.
- No utilice palabras comunes del diccionario como "contraseña", "iloveyou", etc.
- No utilice secuencias como "abcd1234" ni secuencias de teclado como "qwerty".

GESTIÓN DE CONTRASEÑAS:

- Sólo la deben conocer el administrador de la cuenta y otra persona más, por contingencia si la primera no está disponible.
- Utilice una contraseña distinta para cada red social y para los correos electrónicos asociados.
- Mantenga su contraseña en un lugar seguro. Considere usar un software de administración de contraseñas para almacenar toda su información de inicio de sesión de forma segura. Existen las aplicaciones gestoras de contraseñas como, por ejemplo: KeyPass, 1password, Dashlane, Keeper, Roboform, Lastpass, Remembear, Sticky Password, Intuitive Password, Logmeonce.
- Revise y actualice la contraseña y la información de recuperación cuando un miembro del personal deje de trabajar en la empresa.
- Cambie cada tres meses la contraseña de cada una de sus redes y correos asociados.
- Nunca dé su nombre de usuario y contraseña a terceros, especialmente a aquellos que prometen conseguir seguidores, ganar dinero o verificar su identidad.

Doble factor de autenticación

La autenticación en dos pasos es una función de seguridad que, junto a la contraseña, ayuda a proteger la cuenta. Si configura esta función, se le pedirá que ingrese un código de inicio de sesión especial o que confirme el intento de inicio de sesión cada vez que alguien quiera acceder desde un navegador o un celular que no se use habitualmente. También puede recibir alertas cuando alguien intente iniciar sesión desde un navegador o un dispositivo móvil no reconocido.

Enlaces, *phishing* o ingeniería social

Tenga cuidado con los enlaces sospechosos, no abra links sobre los cuales no tenga plena certeza de que se trata de una página segura, incluso cuando se reciben desde una cuenta conocida. Es común que los *hackers* intenten pasarse por alguien cercano o por una empresa para engañar y robar su cuenta o información personal. Esto se conoce como *phishing* o ingeniería social.

Actualizaciones

Asegúrese de que el *software* de su computador y equipo celular, incluido su navegador, esté actualizado con las versiones más recientes.

Antivirus

Instale un programa de antivirus y escanee su computador con regularidad en busca de virus, spyware y adware. Los cortafuegos (*firewalls*, en inglés) son aplicaciones de seguridad que vigilan el tráfico entrante y saliente de la conexión a Internet para proteger el sistema. Generalmente, los antivirus comerciales populares vienen de fábrica con uno, así que lo más sencillo es instalar un buen antivirus y activar su cortafuego.

Aplicaciones seguras

Antes de conectarse a una aplicación se comprobará que sea segura para no comprometer la seguridad de la cuenta. Si se requiere descargar alguna, lo mejor es hacerlo desde tiendas oficiales como Google Play Store o App Store. No hacerlo puede poner en peligro la información e integridad del dispositivo.

Copias de seguridad

Conviene hacer una copia de seguridad, por lo menos una vez al mes, de los datos almacenados, algo que también será de ayuda en casos de robo o pérdida del dispositivo.

Cifrado de datos

No intercambiar información sensible sin encriptar. Tenga en cuenta que, al fin y al cabo, esa información quedará almacenada, así como se intercambió, sin encriptar, en el servidor de una empresa que no se puede gestionar. Para encriptar siga los siguientes pasos:

- Abra el archivo que quiere proteger
- Vaya al apartado “Archivo” en la esquina superior izquierda
- Abra Información
- Haga clic en “Proteger documento”
- Elija la opción “Cifrar con contraseña”
- Escriba una clave

Desconexión de dispositivos

La mayoría de las infecciones suceden cuando el dispositivo está conectado a la red, ya que el *malware* (software malicioso) realiza sus acciones comunicándose con servidores o remitiendo información utilizando puertos abiertos en su conexión. Por ello, es recomendable desconectar la conexión *Wi-Fi* cuando esté utilizando el ordenador para otros propósitos y también antes de apagarlo.

Cierre de sesión

Aunque es más cómodo mantener abiertas las sesiones en la mayoría de las aplicaciones, para no tener que escribir nuevamente el nombre de usuario y contraseña, esto no es recomendable. Lo ideal es siempre cerrar sesión para evitar una posible suplantación de identidad o el robo de datos personales por dejar la sesión abierta.

Contratación de terceros

Cuando se requiera la contratación de terceros para temas relacionados con la gestión de redes sociales, se debe exigir, dentro del contrato, el cumplimiento estricto de este protocolo de seguridad.

Actualización del Protocolo

La Dirección de Comunicaciones y la Dirección de Tecnologías de Información realizarán semestralmente una verificación de la aplicación de este protocolo y actualizarán los contenidos que se requieran.

2

Facebook

Capítulo II: Facebook

Esta red social es la más grande y consultada por los usuarios. Allí se encuentra la mayor diversidad de públicos, por tanto, hay que orientar de manera correcta cada publicación. Facebook permite compartir texto, imágenes, videos, *reels*, enlaces, álbumes de fotografías, historias y realizar transmisiones en vivo.

Autenticación en dos pasos

La autenticación en dos pasos es una función de seguridad que, junto a la contraseña, ayuda a proteger la cuenta. Si configura esta función, se le pedirá que ingrese un código de inicio de sesión especial o que confirme el intento de inicio de sesión cada vez que alguien quiera acceder desde un navegador o un celular que no se use habitualmente. También puede recibir alertas cuando alguien intente iniciar sesión desde un navegador o un dispositivo móvil no reconocido.

Cómo activar o administrar la autenticación en dos pasos

⇒ Desde la cuenta que administra la página de Facebook, vaya a la parte superior derecha, despliegue el menú y dé clic en configuración y privacidad (imagen 1)

Imagen 1

⇒ Después haga clic en *Configuración rápida de seguridad* (imagen 2)

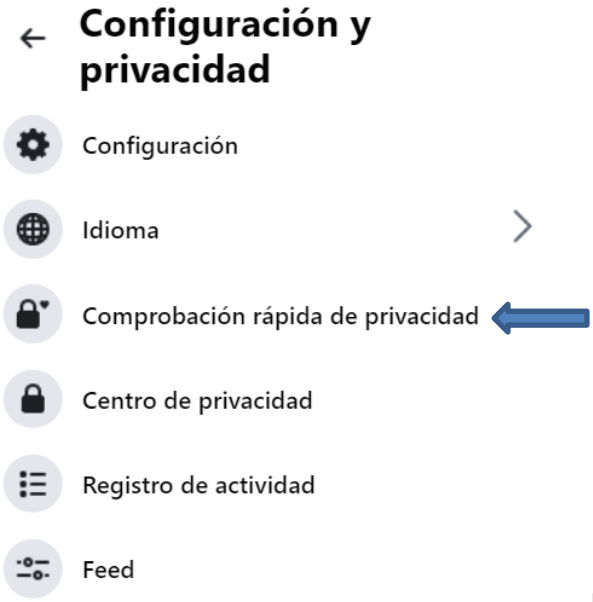


Imagen 2

⇒ En el mosaico acceda a la opción de *Cómo proteger tu cuenta*. (Imagen 3)

Imagen 3

⇒ Dé clic en siguiente, hasta llegar la opción de *Segundo factor de autenticación (Imagen 4)*.

Imagen 4

⇒ Elija el método de seguridad *Autenticación en dos pasos* y siga las instrucciones que aparecen en pantalla. (Imagen 5)

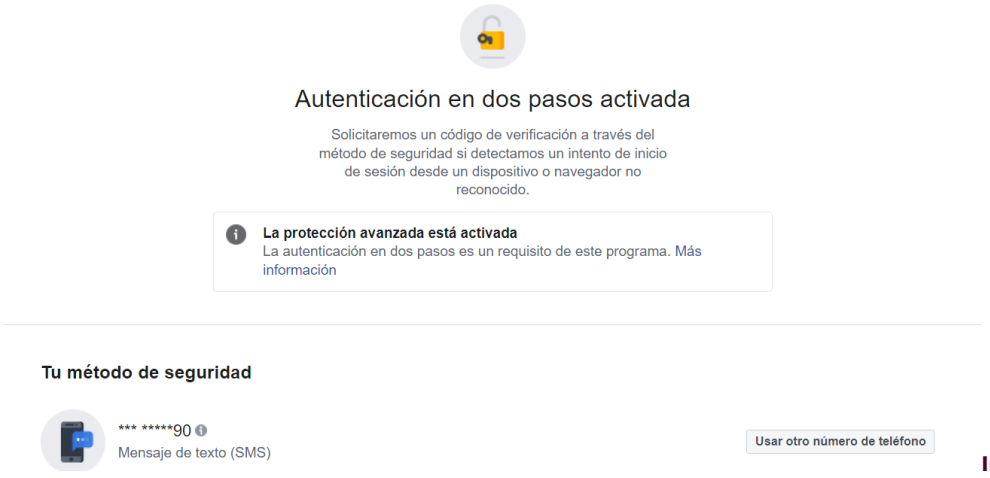


Imagen 5

⇒ Cuando configure la autenticación en dos pasos, se solicitará que elija uno de los tres métodos de seguridad: (Imagen 6)

⇒ Ingresar su clave de seguridad en un dispositivo compatible.

⇒ Códigos de inicio de sesión de una app de autenticación de terceros.

⇒ Códigos de mensajes de texto (SMS) del teléfono celular.

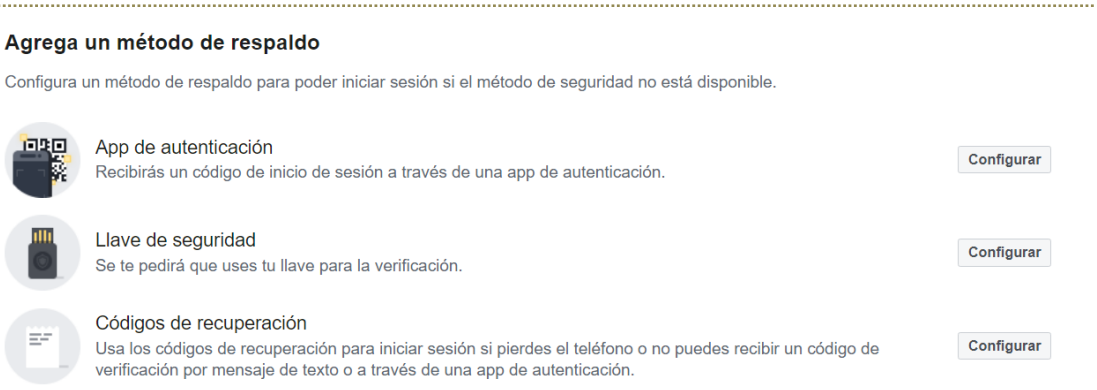


Imagen 6

Roles de Página

Asegúrese de familiarizarse con los diferentes roles de página que existen y los permisos que cada uno concede. Se recomienda revisar con regularidad quién tiene acceso de administrador en la configuración. Además, cuando agregue su página al administrador comercial, dedique un momento a conocer los permisos que otorga. También se recomienda que haya un administrador de contingencia en su página, de modo que, si alguna vez pierde acceso a ella, alguien de confianza pueda seguir manteniendo la página activa y agregarlo de nuevo.

Hay seis tipos de roles para quienes administran páginas. Cuando una persona crea una página, automáticamente se convierte en su administrador, lo que significa que puede cambiar su aspecto y publicar en su nombre. Solo los administradores pueden asignar roles y cambiar los roles de otras personas.

Tenga en cuenta que varias personas pueden tener roles en una página, pero cada una necesita su propia cuenta personal de Facebook.

En la siguiente imagen, se muestran los 6 roles de página y qué pueden hacer:

Rol de página clásico	Acceso a la página en la nueva experiencia para páginas
Administrador	Acceso a Facebook con control total
Editor	Acceso a Facebook con control parcial
Moderador	Acceso a tareas para administrar las respuestas a mensajes, la actividad en la comunidad, los anuncios y las estadísticas
Anunciante	Acceso a tareas para administrar los anuncios y las estadísticas
Analista	Acceso a tareas para administrar las estadísticas
Community manager	Acceso de community manager para moderar chats en vivo

ACCESO A FACEBOOK

Las personas pueden tener acceso a Facebook con control total o control parcial. Pueden acceder a la cuenta de la página y administrarla en Facebook o mediante otras herramientas de Facebook. **Las personas que tienen acceso a Facebook con control total o parcial pueden administrar lo siguiente:**

Contenido: crear, administrar y eliminar contenido en la página, como las publicaciones, las historias y mucho más. Solicitar permiso y acceso para administrar los derechos de tu contenido original y, potencialmente, monetizarlo.

Mensajes: responder mensajes directos en la bandeja de entrada en nombre de la página.

Comentarios: responder comentarios en la página y editar o eliminar comentarios ya hechos por la página.

Cuentas vinculadas: agregar, administrar o eliminar cuentas vinculadas, como una cuenta de Instagram.

Anuncios: crear, administrar y eliminar anuncios.

Estadísticas: usar estadísticas de la página, las publicaciones y los anuncios para analizar el rendimiento de la página.

Eventos: crear, editar y eliminar eventos de la página.

Eliminaciones y prohibiciones: eliminar a personas de la página o prohibir su acceso a ella.

Además, las personas que tienen acceso a Facebook con control total pueden administrar lo siguiente:

Configuración: administrar y editar todas las opciones de configuración, como la información de la página, y eliminar la página.

Acceso: otorgar o eliminar el acceso de las personas a Facebook o a las tareas de la página o de la cuenta de Instagram vinculada, incluido el acceso a Facebook con control total.

Tenga en cuenta que, si decide otorgar acceso a Facebook con control total a otras personas, tendrán el mismo acceso que usted. Esto significa que podrán otorgar acceso a otras personas para que administren la página, eliminar a cualquier persona de la página (incluso a usted) o eliminar la página.

Acceso a tareas

Las personas con acceso a tareas pueden administrar la página mediante otras herramientas de administración, como Meta Business Suite, Creator Studio, el administrador de anuncios o el administrador comercial. Esto quiere decir que no pueden acceder a la cuenta de la página ni administrarla en Facebook. Las personas con acceso a tareas pueden administrar lo siguiente:

Contenido: crear, administrar y eliminar contenido en la página, como las publicaciones, las historias y mucho más. Solicitar acceso a métodos para administrar los derechos de tu contenido original y, potencialmente, monetizarlo.

Mensajes y actividad de la comunidad: responder mensajes directos en la bandeja de entrada en nombre de la página, hacer comentarios, administrar contenido no deseado y reportar actividad en la página.

Anuncios: crear, administrar y eliminar anuncios, y realizar otras tareas relacionadas con ellos.

Estadísticas: ver el rendimiento de la página, del contenido, de los anuncios y de otras métricas.

Acceso de community manager

Los community managers tienen acceso a la moderación del chat de los *streams* en vivo de la página. No pueden acceder a la cuenta de la página ni administrarla en Facebook. Los community managers pueden moderar los chats en vivo de la siguiente manera:

- Eliminar o reportar comentarios.
- Suspender por 15 minutos a usuarios del chat del *stream* en vivo.
- Bloquear usuarios del *stream* en vivo actual o de todos los *streams* en vivo de la página.
- Fijar comentarios en la parte superior del chat en vivo.

Cómo asignarle un rol a una persona

Si es administrador:

⇒ Inicie sesión en Facebook y, luego, haz clic en la foto del perfil en la parte superior derecha y haga clic en *Ver todos los perfiles* y seleccione la página a la que quieras cambiar (Imagen 7)

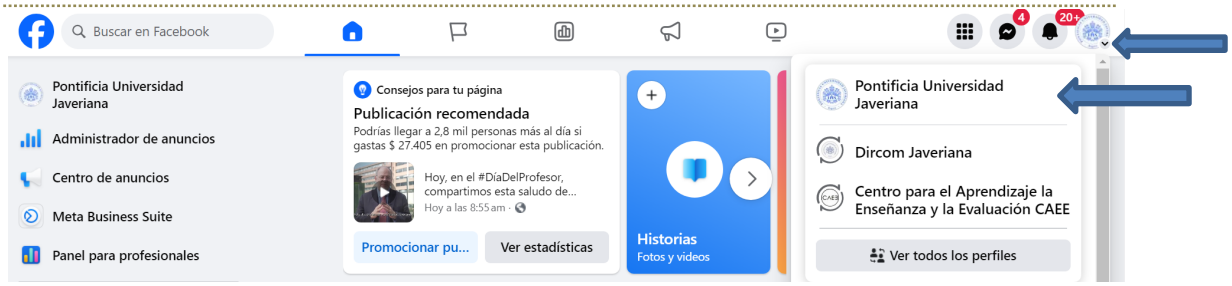


Imagen 7

⇒ Haga clic en Configuración y privacidad y, luego, en Configuración. (Imagen 8)

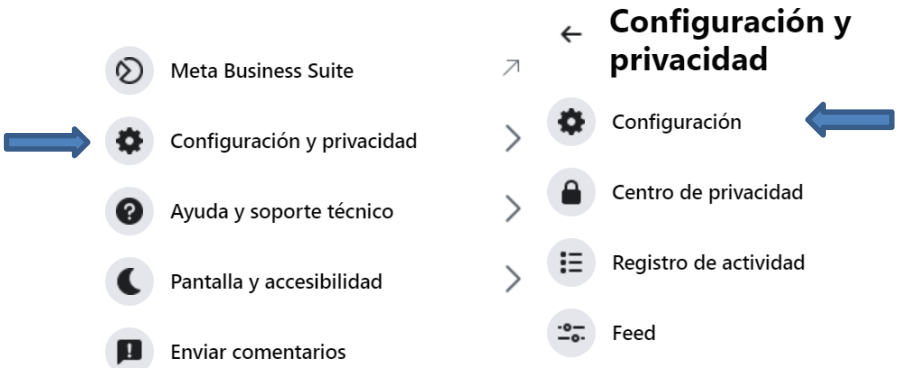


Imagen 8

⇒ En el menú de la izquierda, haga clic en Configuración de la página y luego en Ver junto a Acceso a la página. (Imagen 9)

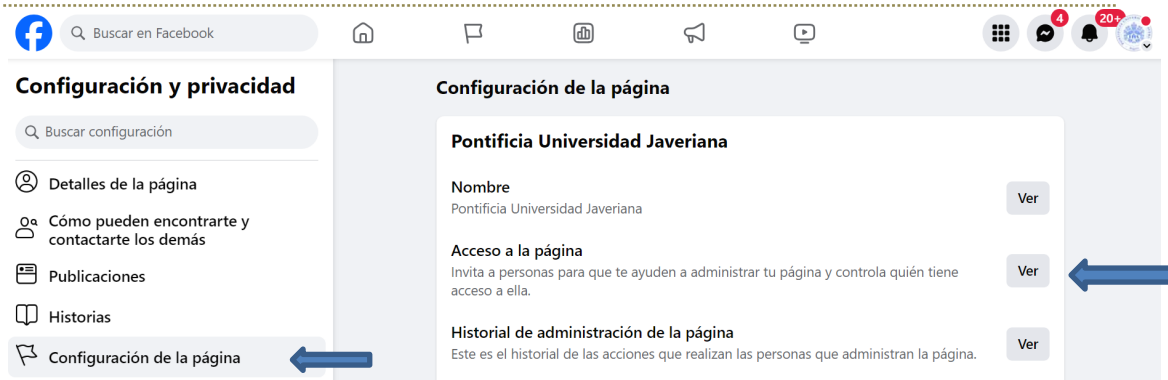


Imagen 9

⇒ Junto a Personas con acceso a Facebook, haga clic en Agregar. (Imagen 10)

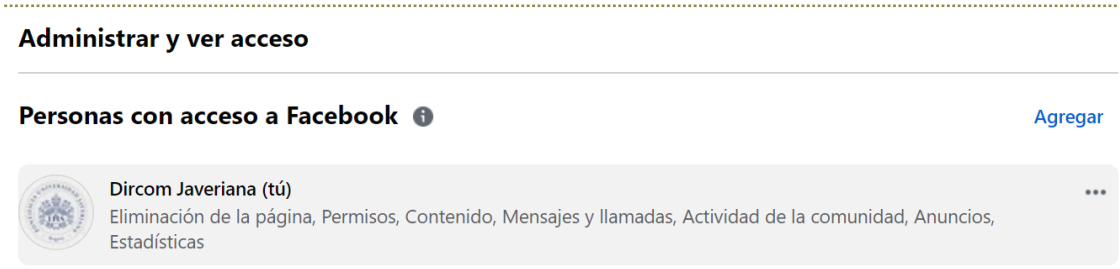


Imagen 10

⇒ Haga clic en Siguiente, escribe el nombre o la dirección de correo electrónico de la persona a la que quieres otorgar acceso a Facebook y haga clic en su nombre. (Imagen 11)

Imagen 11

⇒ Desde aquí, puede elegir otorgar acceso a Facebook con control total o parcial:

- Para otorgar acceso a Facebook con control parcial: desplácese hacia abajo y haga clic en Otorgar acceso.
- Para dar acceso a Facebook con control total: desplácese hacia abajo, arrastre para que la persona tenga control total y, luego, haga clic en Otorgar acceso.
- Escriba su contraseña de Facebook y haga clic en Confirmar.

CÓMO ELIMINAR A UNA PERSONA QUE TIENE UN ROL

Si es administrador:

⇒ Siga los mismos pasos de Cómo asignarle un rol a una persona. Cuando llegue a la sección Personas con acceso a Facebook, haga clic en los tres puntos al lado del usuario que desea eliminar. (Imagen 12)

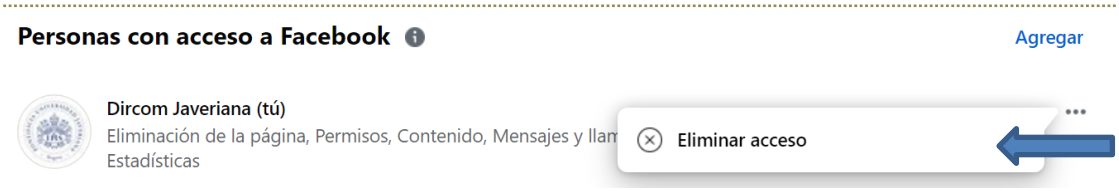


Imagen 12

⇒ Escriba su contraseña y haga clic en confirmar. (Imagen 13)

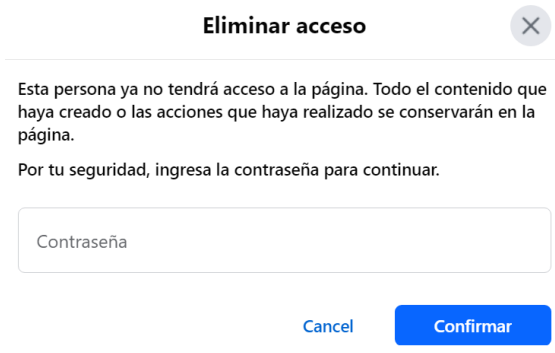


Imagen 13

- **Nota:** Puede eliminarse de una página en cualquier momento, pero primero debe agregar a otro administrador si es el único administrador de la página. Si quiere eliminar a otro administrador, tal vez sea necesario que el administrador en cuestión apruebe su solicitud para poder hacerlo.

CÓMO CAMBIAR EL NIVEL DE ACCESO DE UNA PERSONA O EDITAR TAREAS

Si es administrador:

⇒ Siga los mismos pasos de Cómo asignarle un rol a una persona. Cuando llegue a la sección Personas con acceso a Tareas, haga clic en los tres puntos al lado del usuario que desea modificar. (Imagen 14)

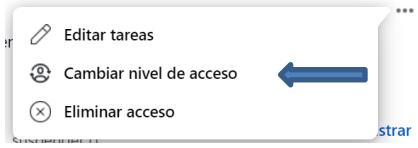


Imagen 14

⇒ Para editar tareas, seleccione los permisos que desea agregar o eliminar. (Imagen 15 y 16)

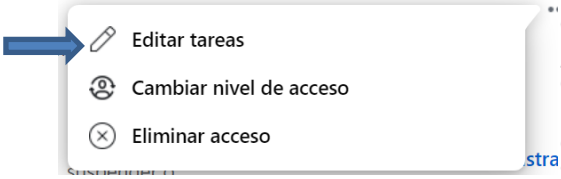


Imagen 15

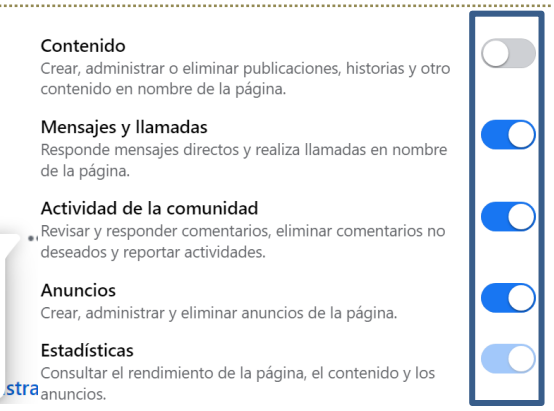


Imagen 16

Nota: Si hay varias personas con roles de administración o edición de la página, se puede verificar quién realizó determinada publicación de las siguientes maneras:

- En una publicación de página, el nombre de la persona aparece junto a Publicado por.
- En cada comentario de la página, el nombre de la persona aparece debajo del comentario, junto a Comentado por.
- Haga clic en Herramientas de publicación en la parte superior de la página. En la columna de la izquierda, haga clic en Publicaciones realizadas, Publicaciones programadas o Borradores para ver quién escribió un borrador, quién publicó o programó publicaciones de la página.
- También puede ver quién publicó o programó publicaciones en el registro de actividad de la página.

Tu Actividad

⇒ El registro de actividad te permite revisar y administrar lo que compartes en Facebook.

VER EL REGISTRO DE ACTIVIDAD

Haga clic en tu foto del perfil en la parte superior derecha de Facebook. Seleccione Configuración y privacidad y, luego, haga clic en Registro de actividad.
Allí, puede filtrar los resultados por Fecha o revisar los Tipos de actividad, por ejemplo:

- Sus publicaciones para revisar fotos, videos, texto y actualizaciones de estado que compartiste en Facebook.
- Actividad en la que te etiquetaron para revisar publicaciones, fotos y comentarios en los que te hayan etiquetado.
- Interacciones para revisar Me gusta, reacciones y comentarios.

- Grupos y eventos para revisar la actividad en tus grupos y los eventos que creaste.
- Información del perfil para revisar tu número de teléfono y tu dirección de correo electrónico.
- Conexiones para revisar amigos, páginas que te gustan y relaciones.
- Acciones registradas y otra actividad para revisar tus dispositivos, inicios de sesiones y videos que viste.

APPS Y SITIOS WEB

Estas son apps y sitios web que conectó a su cuenta de Facebook al iniciar sesión en ellos con Facebook o al conectar una cuenta que tiene en su plataforma con su cuenta de Facebook. Puede revisar y administrar la información no pública a la que cada app tiene permiso para acceder o bien eliminar su acceso.

⇒ Vaya a la cuenta con la cual administra la página de Facebook y haga clic en Configuración de Privacidad. (Imagen 17)

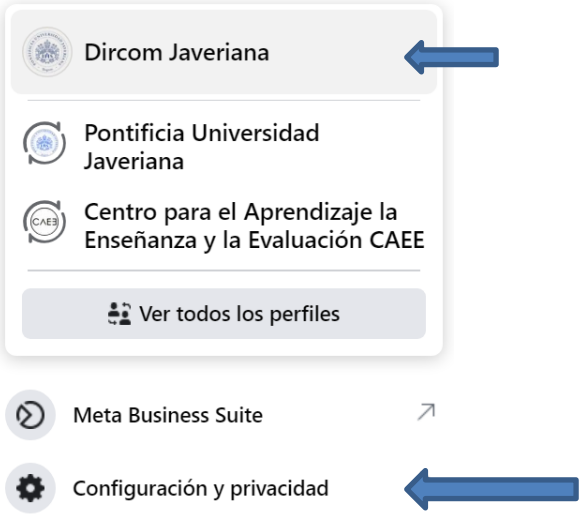


Imagen 17

⇒ Seleccione Configuración. (Imagen 18)

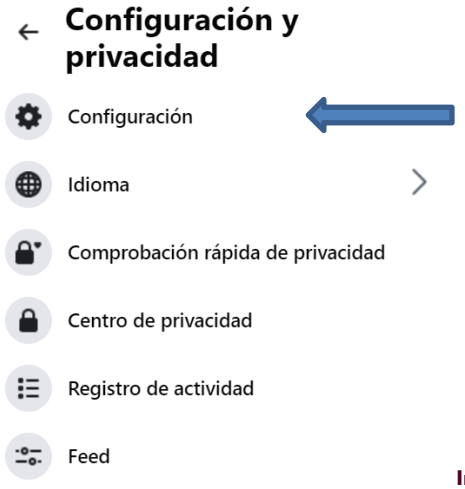

Configuración y privacidad
Configuración
Idioma
Comprobación rápida de privacidad
Centro de privacidad
Registro de actividad
Feed

Imagen 18

⇒ En Apps y sitios web, elimine las apps conectadas a su cuenta que no esté usando. (Imagen 19)

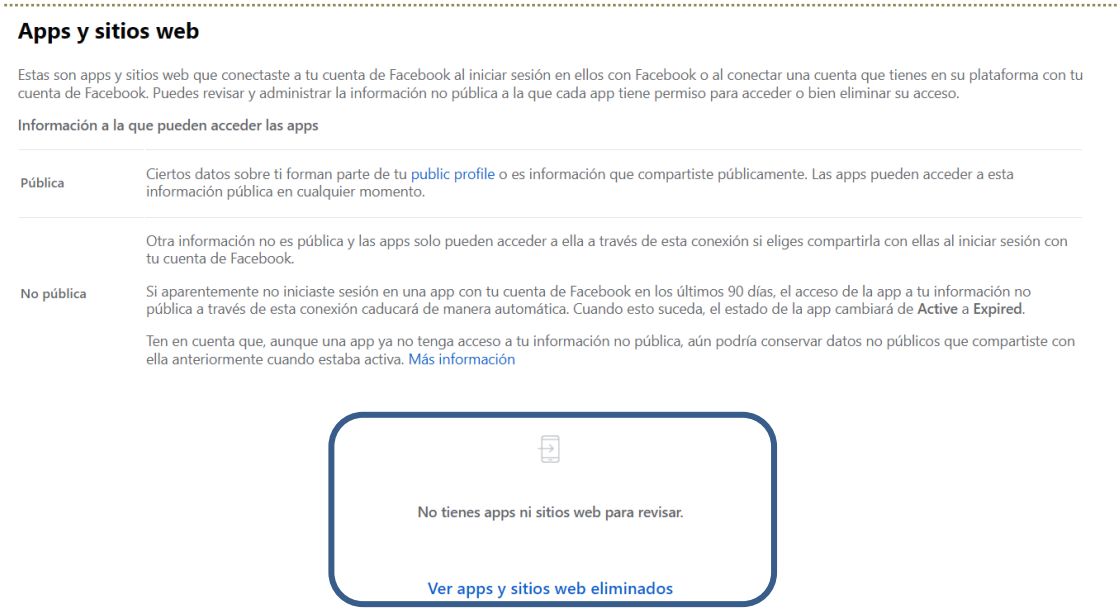


Imagen 19

PREFERENCIAS

⇒ Siga los mismos pasos anteriores (Apps y Sitios Web), deslice hasta Preferencias y desactive las opciones *Apps, sitios web y juegos* y Notificaciones de juegos y apps. (Imagen 20)

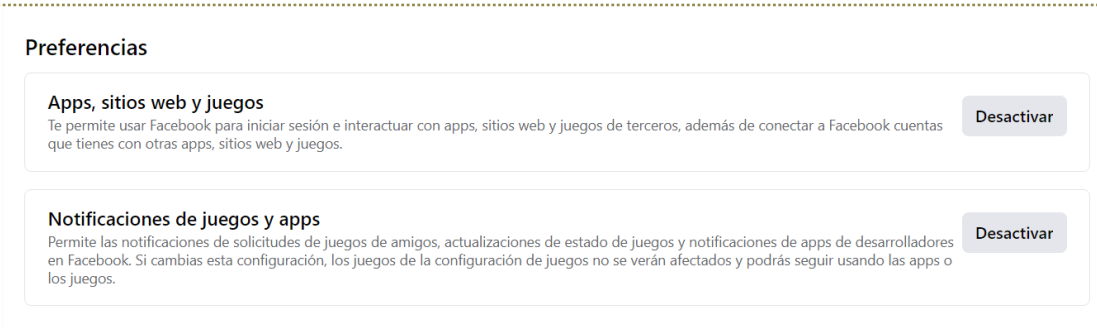


Imagen 20

Consejos y funciones de seguridad

Use las funciones de seguridad de Facebook, las aprobaciones y las alertas de inicio de sesión, y revise y actualice su configuración de seguridad en cualquier momento.

Proteja su cuenta de Facebook

Estas son algunas medidas que puede tomar para proteger su cuenta.

Proteja su contraseña.

- No utilice su contraseña de Facebook en ningún otro lugar de internet ni la compartas nunca.
- Su contraseña debe ser difícil de adivinar, así que no incluya su nombre ni palabras comunes.
- Más información sobre cómo crear una contraseña segura.

Nunca comparta su información de inicio de sesión.

- Los estafadores pueden crear sitios web falsos que se parezcan al de Facebook y pedirle que inicie sesión con su correo electrónico y contraseña.
- Antes de ingresar su información de inicio de sesión, siempre compruebe la URL del sitio web. Si tiene dudas, escriba www.facebook.com en la barra del navegador para ir a Facebook.
- No reenvíe correos electrónicos de Meta a otras personas, ya que pueden contener información confidencial sobre su cuenta.
- Obtenga sobre cómo evitar el phishing.

Cierre sesión en Facebook cuando utilice una computadora que comparta con otras personas.

- Si se olvida de hacerlo, puede cerrar la sesión de forma remota.

No acepte solicitudes de amistad de personas que no conozcas.

- Los estafadores pueden crear cuentas falsas para conseguir amigos.
- Si se hace amigo de estafadores, podría permitirles que publiquen spam en su biografía, lo etiqueten en publicaciones y le envíen mensajes malintencionados.

Tenga cuidado con el software malicioso.

- El software malintencionado puede causar daños a una computadora, un servidor o red de computadoras.
- Obtenga información sobre los indicios de una computadora o un dispositivo infectados y sobre cómo puede eliminar software malicioso.
- Mantenga su navegador actualizado y elimine apps y complementos del navegador que resulten sospechosos.

Nunca haga clic en enlaces sospechosos, aunque procedan de un amigo o de una empresa que conoces.

- Este consejo se aplica también a enlaces en Facebook (por ejemplo, en publicaciones) o en correos electrónicos.
- Tenga en cuenta que Meta nunca te enviará un correo electrónico para pedirte tu contraseña.
- Si ve un enlace sospechoso en Facebook, repórtalo.

Administrar tus alertas y métodos de autenticación

Recibe alertas sobre inicios de sesión no reconocidos en Facebook

- Haga clic en su foto del perfil en la parte superior derecha y, luego, haga clic en Configuración y privacidad.
- Haga clic en Configuración.
- Haga clic en Centro de cuentas y, luego, en Contraseña y seguridad.
- Haga clic en Alertas de inicio de sesión.
- Elija cómo quiere recibir las alertas, por ejemplo, en su cuenta de correo electrónico o mediante una notificación de Facebook desde un dispositivo reconocido.

Una vez que empiece a recibir alertas acerca de inicios de sesión no reconocidos:

- Cuando reciba una alerta de inicio de sesión, puede indicar si reconoce la actividad de inicio de sesión seleccionando o tocando Fui yo.
- Si no reconoce la actividad de inicio de sesión, seleccione o toque No fui yo y Facebook le ayudará a restablecer la contraseña y proteger la cuenta.
- Puede guardar un dispositivo o un navegador en tu lista de navegadores de confianza o dispositivos reconocidos. De esta manera, no recibirá alertas relacionadas con la computadora o el dispositivo móvil que utiliza habitualmente para iniciar sesión en Facebook. No seleccione esta opción si usa una computadora pública (por ejemplo, en una biblioteca o una cafetería).
- Puede encontrar una lista de dispositivos recientes que iniciaron sesión en su cuenta de Facebook en la configuración de seguridad e inicio de sesión.

Evitar spam y estafas

Administrar el spam en Facebook

El spam implica ponerse en contacto con otras personas con contenido o solicitudes no deseados. Este término engloba el envío de mensajes en masa, la publicación excesiva de enlaces o imágenes en las biografías de otras

personas y el envío de solicitudes de amistad a personas que no conoce

El spam puede propagarse cuando se hace clic en enlaces no seguros o se instala software malicioso. En ocasiones, los estafadores obtienen acceso a las cuentas de Facebook de las personas y las utilizan para enviar spam.
Si hizo clic en algo que resultó ser spam o si su cuenta está creando publicaciones, eventos, grupos o páginas no deseados, pruebe con estos pasos:

Revise la actividad de la cuenta y elimina todo el spam

⇒ Compruebe si hay inicios de sesión sospechosos en el historial de inicios de sesión. Vaya a la foto de perfil de su cuenta y haga clic en Configuración y Privacidad. (Imagen 20)

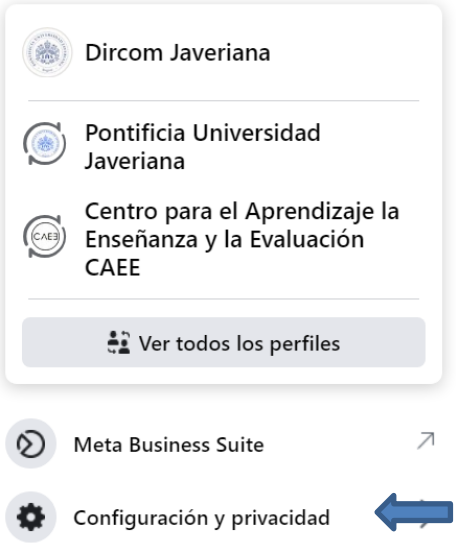


Imagen 20

⇒ Haga clic en Registro de actividad (Imagen 21)

Imagen 21

⇒ Deslice hasta la opción Dónde iniciaste sesión. (Imagen 22)

Imagen 22

⇒ Elimine los inicios de sesión que no reconozca. (Imagen 23)

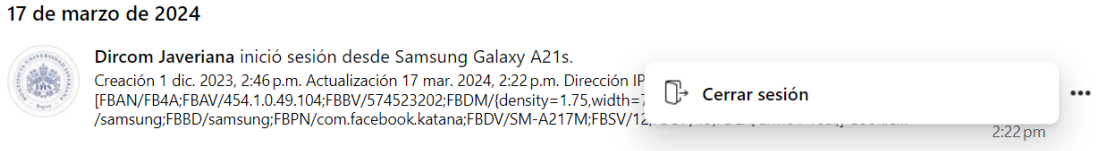


Imagen 23

- Revise sus publicaciones y Me gusta recientes.
- Consulte su registro de actividad y elimine las acciones no deseadas.
- Revise sus apps y juegos instalados, y elimina todo el contenido en el que no confíes.
- Elimine cualquier foto, publicación, página, grupo o evento que no hayas creado.

Filtro de groserías en Facebook

Si ayuda a administrar una página de Facebook, puedes usar el filtro de groserías para ocultar en ella comentarios con groserías. Facebook determina qué se debe ocultar en función de

las palabras y las frases que más se reportan en la comunidad por ser ofensivas. Los comentarios ocultos por tener esas palabras siguen siendo visibles para quienes los escribieron y sus amigos. pero no para los demás.

ACTIVAR Y DESACTIVAR EL FILTRO DE GROSERÍAS EN FACEBOOK

- Inicie sesión en Facebook y, luego, haga clic en tu foto del perfil en la parte superior derecha.
- Haga clic en Ver todos los perfiles y seleccione la página a la que quiera cambiar.
- Haga clic en la foto de la página en la parte superior derecha y, luego, en Configuración y privacidad.
- Haga clic en Configuración y, luego, haga clic en Seguidores y contenido público.
- Haga clic en junto a Ocultar publicaciones y comentarios con groserías para activar la opción, o bien haga clic en para desactivarla.

⇒ También puede moderar de forma proactiva los comentarios de las personas que visitan la página bloqueando palabras y activando el filtro de groserías[2]. (Imagen 24)

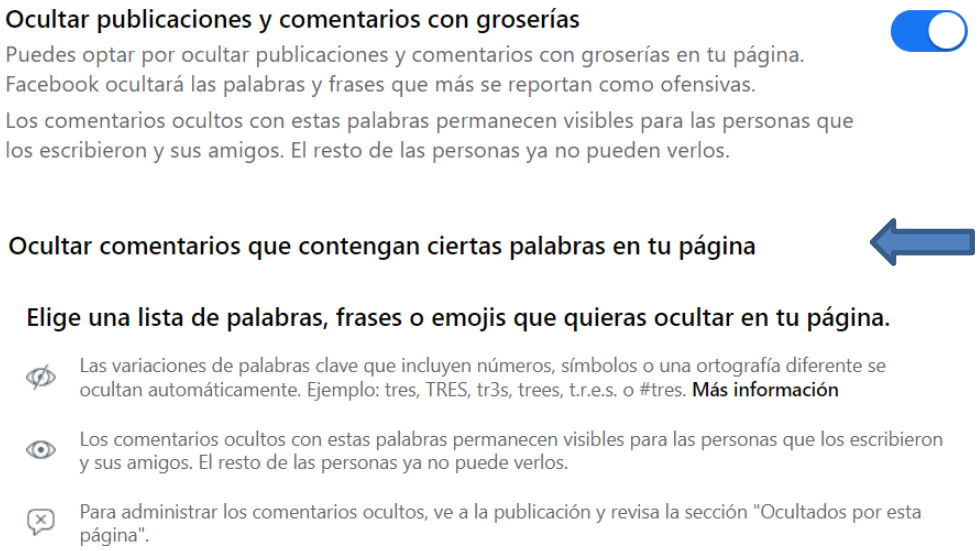


Imagen 24

[2] Aquí puede descargar el documento "Palabras prohibidas en redes sociales" en formato CSV para adjuntarlo al filtro de groserías: https://intranet.javeriana.edu.co/web/rectoria/area-gestion-redes-sociales-y-streaming

Controles de seguridad automáticos:

CONTROL DE LINKS

Función de Facebook con la que, con el apoyo de fabricantes de softwares y antivirus, se cotejan cerca de 2 billones de enlaces a diario para que el spam se reduzca al 0.5% de los usuarios.

ELIMINACIÓN DE SPAM

La seguridad de Facebook elimina los posts de noticias y titulares que llaman la atención para que uno haga clic (clickbait).

COMPROBACIÓN DE CLICS EN EL BOTÓN "ME GUSTA"

Facebook identifica páginas sospechosas y le pregunta al usuario si realmente hizo clic conscientemente en ese like.

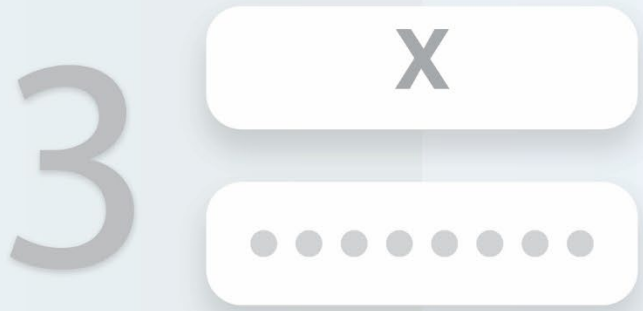
POSIBLE SECUESTRO DE LA CUENTA

Lo primero que se recomienda es cerrar todas las sesiones abiertas siguiendo las siguientes instrucciones:

https://web.facebook.com/help/211990645501187?_rdc=1&_rdr

Si el problema continúa, se sugiere, por seguridad, solicitar el bloqueo de la misma en la opción: https://www.facebook.com/help/1216349518398524/?helpref=hc_fnav

3



Capítulo III: X

X es una plataforma social bidireccional, cuyo objetivo es compartir información de forma rápida y sencilla. Desde el año 2023, implementó la opción de verificación para creadores de contenidos y organizaciones. Estas dos versiones son pagas.

Su éxito se basa en la inmediatez de mensajes cortos, lo que la hace una red social para leer y escribir muy rápido. En el ámbito institucional, X permite divulgar noticias, eventos, servicios, entre otros.

Cabe recordar que es una red muy interactiva, para público externo y que las publicaciones no deben sobrepasar los 280 caracteres, si no se está suscrito a la versión Premium.

Restablecer contraseña

Si olvidó la contraseña o perdió acceso a la cuenta, puede reestablecerla siguiendo estos pasos:

⇒ Ingresar a x.com

⇒ Escribir el nombre de la cuenta, correo electrónico o número de celular asociado

⇒ Hacer clic en *Olvidé mi contraseña* (Imagen 1)

Imagen 1

⇒ Si reconoce el correo electrónico o el número de celular, activarlo y dar clic en siguiente. Le llegará un código por mensaje de texto o al correo asociado con el cual podrá cambiar la contraseña y recuperar la cuenta.

⇒ Si no tiene acceso al correo electrónico o al número de celular que aparecen allí, dar clic consulte más información en el Centro de ayuda.

Autenticación de dos factores

Con esta opción, en lugar de ingresar solo una contraseña para iniciar sesión, también se debe ingresar un código o una clave de seguridad. Este paso adicional ayuda a garantizar que nadie más acceda a su cuenta.

Después de habilitar esta función, necesitará la contraseña y un método de inicio de sesión secundario, que puede ser un mensaje de texto (sólo disponible para la versión premium paga), un código, una confirmación de inicio de sesión a través de una aplicación o una llave de seguridad física que se conecta al dispositivo a través de USB (también conocidas como claves de seguridad U2F o claves de seguridad de *hardware*) para iniciar sesión.

CÓMO VERIFICAR EL INICIO DE SESIÓN

⇒ En el menú lateral, haga clic en *Más opciones* (Imagen 2)

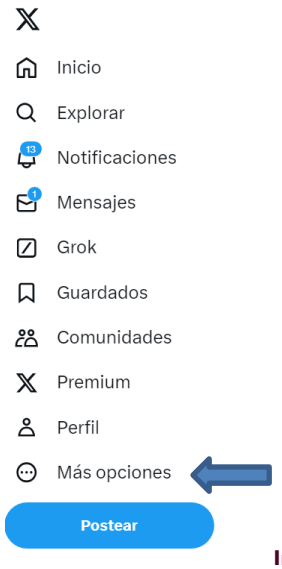


Imagen 2

⇒ Luego haga clic en *Configuración y privacidad*. (Imagen 3)

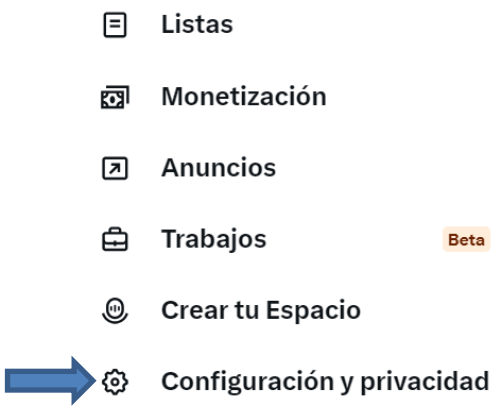


Imagen 3

⇒ Haga clic en Seguridad y acceso a la cuenta, y luego en Seguridad. (Imagen 4)

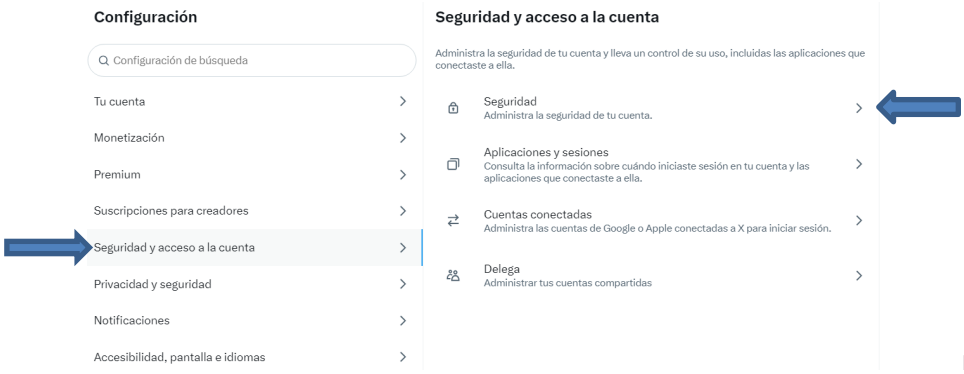


Imagen 4

⇒ Haga clic en Autenticación en dos fases. (Imagen 5)

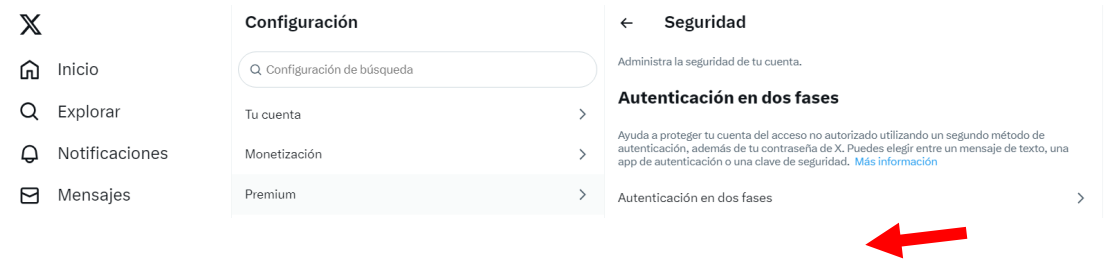


Imagen 5

⇒ Podrá elegir entre tres métodos: Mensaje de texto (únicamente para versión Premium), Aplicación de autenticación o Clave de seguridad. (Imagen 6)

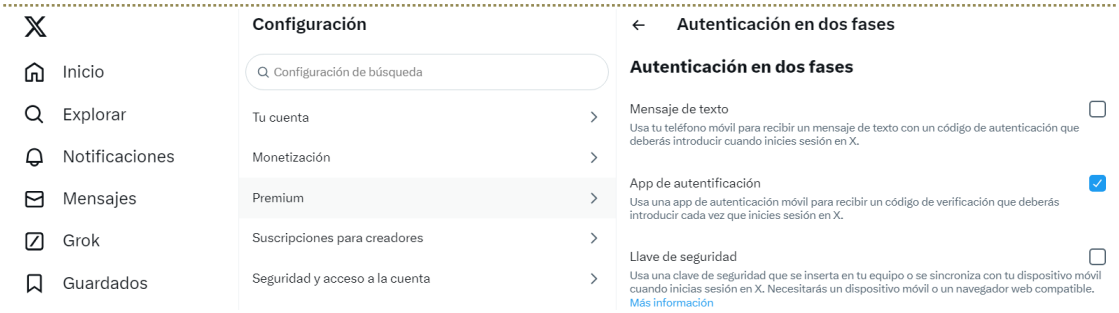


Imagen 6

Nota: Por recomendación de la Dirección de Tecnologías de la Información de la Pontificia Universidad Javeriana, para cuentas que no son Premium, se recomienda activar la opción de App de Autenticación de Microsoft Authenticator.

⇒ Una vez realizada la inscripción e iniciada la sesión, se le pedirá que indique el método de autenticación de dos factores que utilizó en su inicio de sesión anterior, junto con la contraseña.

CÓMO REGISTRARSE A TRAVÉS DE LA APLICACIÓN DE AUTENTICACIÓN

⇒ Haga clic en la casilla de verificación junto a *Aplicación de autenticación*. (Imagen 7)

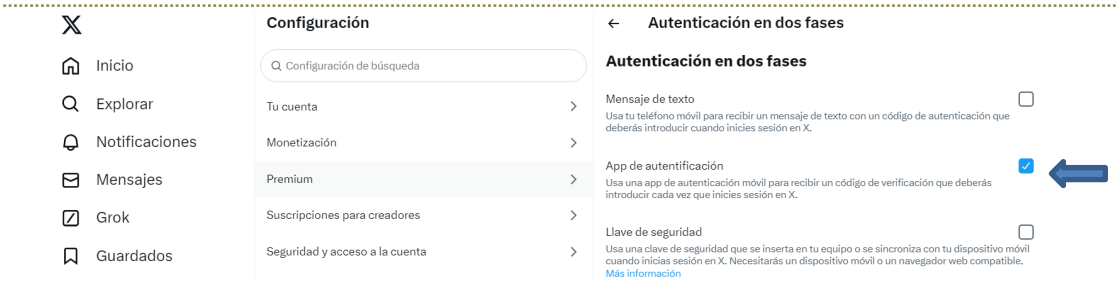


Imagen 7

⇒ Ingrese la contraseña y haga clic en Verificar.

⇒ Se le solicitará que vincule la aplicación de autenticación a la cuenta escaneando un código QR. (Si aún no tiene una aplicación instalada en el dispositivo, deberá descargar una. Puede usar cualquier aplicación de autenticación de contraseña temporal de un solo uso (TOTP), como Google Authenticator o1Password, entre otros. Sin embargo, por sugerencia de la DTI sugerimos Microsoft Authenticator.

⇒ Después de escanear el código QR, haga clic en Siguiente.

⇒ Ingrese el código generado por la aplicación de autenticación y, luego, haga clic en Verificar.

⇒ Verá una pantalla de confirmación. Haga clic en Entendido para finalizar la configuración.

⇒ A través de la aplicación de autenticación, puede ver y usar códigos para iniciar sesión en su cuenta.

CÓMO REGISTRARSE MEDIANTE UNA LLAVE DE SEGURIDAD

Para comenzar, primero necesitará activar uno de los métodos de autenticación de dos factores, ya sea mensaje de texto o aplicación de autenticación.

⇒ Haga clic en Llave de seguridad.

⇒ Cuando se le solicite, ingrese la contraseña.

⇒ Lea las instrucciones generales y, luego, haga clic en Comenzar.

⇒ Puede insertar la(s) llave(s) en el puerto USB de su equipo o sincronizarla(s) a través de Bluetooth o NFC. Una vez que la(s) haya insertado, pulsa el botón en su clave.

⇒ Siga las instrucciones que se indican en pantalla para finalizar la configuración.

⇒ Cuando termine, su(s) llave(s) de seguridad aparecerá(n) en la sección Administrar claves de seguridad debajo de Autenticación de dos factores. Desde allí, puede cambiar el nombre o eliminar su(s) llave(s) de seguridad y agregar llaves de seguridad adicionales a su cuenta en cualquier momento.

Nota 1: Deberá usar la última versión de un navegador compatible, como Chrome, Edge, Firefox, Opera o Safari, para agregar o iniciar sesión en su cuenta con una llave de seguridad. Ahora, con la llave de seguridad, puede iniciar sesión en su cuenta en x.com.

Nota 2: También es posible aprobar o rechazar las solicitudes de inicio de sesión en la aplicación pulsando *Seguridad* y, luego, *Solicitudes de inicio de sesión*. Despliegue la lista para actualizarla y ver solicitudes nuevas. Las solicitudes aparecerán en esta pantalla, incluso si no recibió una notificación *push*.

Códigos de respaldo

CÓMO USAR LOS CÓDIGOS DE RESPALDO

Una vez activada la autenticación de dos factores, se generará un código de respaldo automáticamente. Escriba, imprima o tome una captura de pantalla de este código de respaldo y téngalo en un lugar seguro. En caso de que pierda su celular o cambie de número de teléfono, podrá usar este código de respaldo para iniciar sesión en la cuenta. Una vez, utilice el código de respaldo, deberá generar uno nuevo.

⇒ Vaya a la página de Configuración *y privacidad.* (Imagen 8)

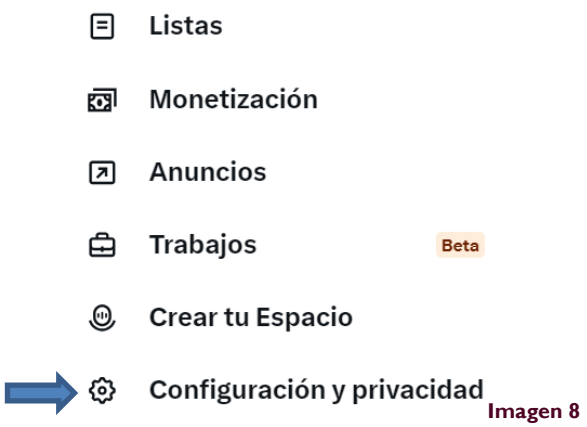


Imagen 8

⇒ Pulse Seguridad y acceso a la cuenta y, luego, Seguridad. (Imagen 9)

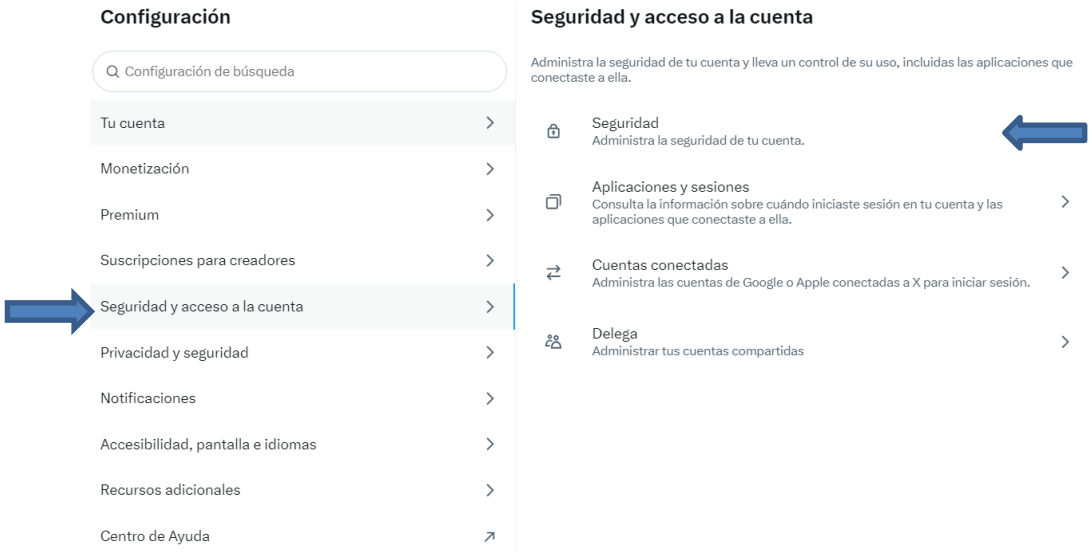


Imagen 9

⇒ Haga clic en Autenticación de dos fases. (Imagen 12)

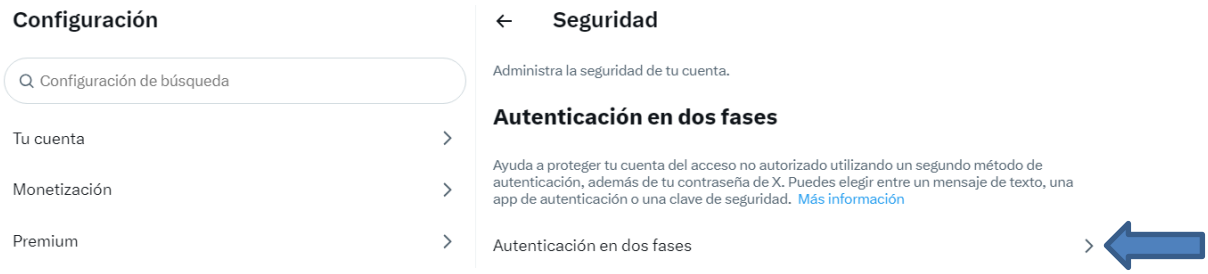


Imagen 12

⇒ Pulse Código de respaldo. (Imagen 13)

Imagen 13

Para usar el código de respaldo, inicie sesión en X con la combinación habitual de nombre de usuario y contraseña. Cuando vea que se envió una solicitud de autenticación de dos factores, haga clic en el vínculo para ingresar el código de respaldo. Ingrese el código de respaldo que generó para iniciar sesión en el sitio.

Nota: Puede generar hasta cinco códigos de respaldo activos en cualquier momento. Asegúrese de usar los códigos en el orden en que los generó; si usa un código fuera de este orden, se invalidarán todos los códigos generados anteriormente.

QUÉ HACER CUANDO SE RECIBE UN ERROR AL USAR LOS CÓDIGOS DE RESPALDO

⇒ Si intenta iniciar sesión con un código de respaldo inactivo o intenta usar un código de respaldo que ya no funciona, verá un mensaje de error. Deberá generar un nuevo código de respaldo para iniciar sesión.

⇒ Los códigos de respaldo solo funcionarán cuando se inicia sesión en x.com, mobile.x.com, X para iOS o Android, u otro cliente de X. Si intenta acceder a una aplicación de terceros asociada a la cuenta de X, deberá usar una contraseña temporal en lugar del código de respaldo.

Pérdida o cambio de celular

QUÉ HACER EN CASO DE PÉRDIDA DEL CELULAR ASOCIADO

⇒ Si activó la autenticación de dos factores y generó un código de respaldo, ingréselo para acceder a la cuenta y actualizar la Configuración móvil.

⇒ Si ya no tiene una sesión abierta en su cuenta y no tiene acceso a un código de respaldo activo, comuníquese con el equipo de soporte de X para solicitar ayuda (https://help.x.com/es).

QUÉ HACER EN CASO DE CAMBIO DEL CELULAR ASOCIADO

⇒ Se sugiere hacer una copia de seguridad del teléfono anterior antes de reemplazarlo. Esto permitirá restaurar la sesión de la aplicación en el dispositivo nuevo para que pueda seguir usando la autenticación de dos factores. (**Nota**: Si es usuario de X para iOS, le recomendamos que realice una copia de seguridad encriptada para conservar la clave de la aplicación. Por lo general, las copias de seguridad de iCloud no conservan la clave; si no cuenta con una copia de seguridad encriptada, es posible que se le pida que inicie sesión de nuevo en la aplicación mediante una contraseña temporal generada en x.com).

- También puede desactivar la autenticación de dos factores en su teléfono anterior o en x.com si tiene una sesión abierta en la web. Si no tiene una sesión web abierta y no tiene su teléfono anterior, igualmente puede iniciar sesión en x.com con el código de respaldo.

QUÉ HACER EN CASO DE NO PODER INICIAR SESIÓN EN EL CELULAR ASOCIADO

⇒ Una solución posible es modificar la sección de configuración del celular. Iniciando sesión en x.com desde un equipo de escritorio o portátil.

⇒ Otra opción es cerrar la sesión de la cuenta desde el dispositivo que se usó para activar la autenticación de dos factores. De esta forma, se podrá iniciar sesión con el nombre de usuario y contraseña.

Aplicaciones de terceros

Si desea otorgar acceso a una aplicación de terceros a su cuenta, le recomendamos que solo lo haga utilizando el método OAuth de X, método de conexión seguro que no requiere entregar nombre de usuario y contraseña al tercero. Se sugiere evitar al máximo usar aplicaciones de terceros. Puede revocar el acceso a aplicaciones que no reconoce o que están publicando en su nombre visitando la pestaña *Aplicaciones* en la configuración de su cuenta.

Aplicaciones y sesiones

APLICACIONES CONECTADAS

Revise periódicamente las aplicaciones que están vinculadas a su cuenta. Deje activas solamente aquellas que utilice para planificación o *social listening*.

⇒ Vaya a Configuración y Privacidad. (Imagen 14)

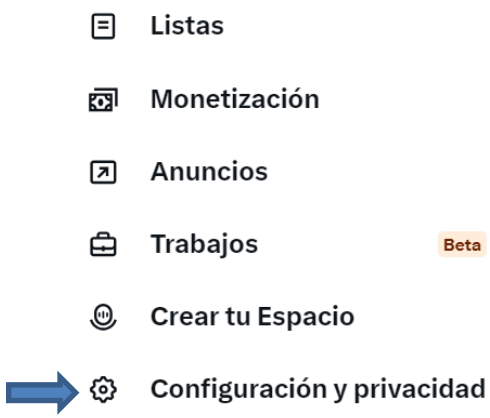


Imagen 14

⇒ Haga clic en Seguridad y acceso a la cuenta y luego en Aplicaciones y sesiones. (Imagen 15)

Imagen 15

⇒ En Aplicaciones conectadas, elimine aquellas que no utilice o que no sean para planificación de contenido.

SESIONES

⇒ Siga los pasos anteriores de Aplicaciones conectadas y seleccione la opción Aplicaciones y sesiones. (Imagen 16)

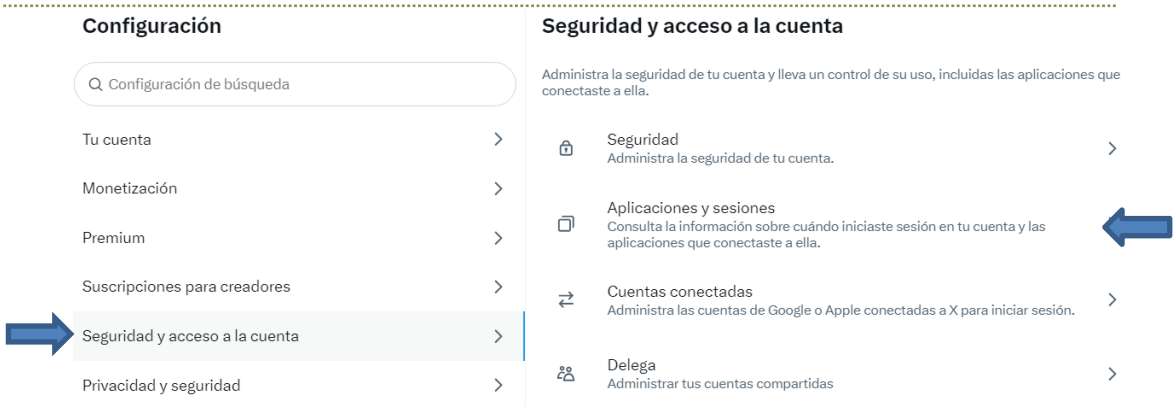


Imagen 16

⇒ Vaya a sesiones y cierre aquellas que no reconozca o que no estén activas por un periodo superior a 15 días. (Imagen 17)

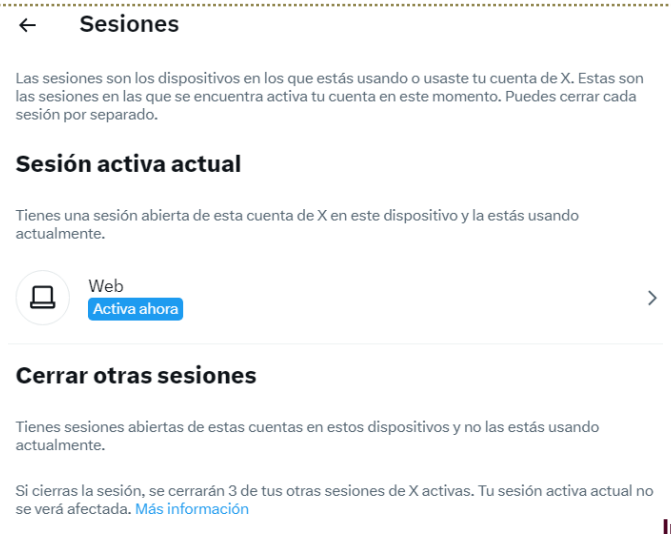


Imagen 16

Controles de seguridad automáticos

CONTRASEÑAS

X nunca le pedirá que proporcione su contraseña por correo electrónico, mensaje directo o respuesta.

ARCHIVOS ADJUNTOS Y ENLACES

X nunca pedirá que descargue algo o que inicie sesión en un sitio web diferente. Nunca abra un archivo adjunto ni instale ningún *software* de un correo electrónico que afirme ser de X Pro.

Intento de *hackeo*

Si X sospecha que su cuenta ha sido pirateada, restablecerá la contraseña para evitar que el *hacker* haga un mal uso de su cuenta. En este caso, enviará un correo electrónico con un enlace para restablecer la contraseña de twitter.com.

Inicio de sesión sospechoso

Si X detecta un inicio de sesión sospechoso enviará una notificación automática dentro de la aplicación o por correo electrónico como una capa adicional de seguridad para su cuenta. Las alertas de inicio de sesión solo se envían después de nuevos inicios de sesión. Con estas alertas, puede verificar que fue usted quien inició sesión desde el dispositivo. Si no inició sesión desde el dispositivo, debe seguir los pasos de la notificación para proteger su cuenta, comenzando por cambiar su contraseña inmediatamente. Tenga en cuenta que la ubicación que aparece en la notificación es una ubicación aproximada derivada de la dirección IP que utilizó para acceder a X, y puede ser diferente de su ubicación física. Si inicia sesión en su cuenta de X desde navegadores de incógnito o navegadores con *cookies* deshabilitadas, recibirá una alerta cada vez.

Cambio de correo

Cada vez que se cambie la dirección de correo electrónico asociada con su cuenta, X le enviará una notificación por correo electrónico a la dirección utilizada anteriormente.

Posible secuestro de la cuenta

Lo primero que se recomienda es cerrar todas las sesiones abiertas siguiendo las siguientes instrucciones: https://x.com/settings/sessions

Si el problema continúa, el Centro de Ayuda de X le brinda una serie de recomendaciones: https://help.x.com/es/managing-your-account/cant-access-my-accounts-email-address

4

Instagram

Instagram es una aplicación móvil que permite a los usuarios compartir fotografías, videos, *reels* e historias con variedad de efectos, marcos, opciones de interacción, entre otros. Actualmente es una de las redes más populares entre jóvenes y adultos jóvenes, por tanto, su buena gestión y calidad en las fotografías puede impactar de manera positiva.

Ajustes de seguridad

La nueva configuración de Instagram, al ser adquirida por la compañía Meta, comparte aspectos de seguridad de Facebook. Para encontrar los ajustes de seguridad:

⇒ Abra el perfil desde su celular.

⇒ Haga clic en las tres barras de la esquina superior derecha de la pantalla. (Imagen 1)

Imagen 1

⇒ Seleccione *Centro de cuentas*. (Imagen 2)

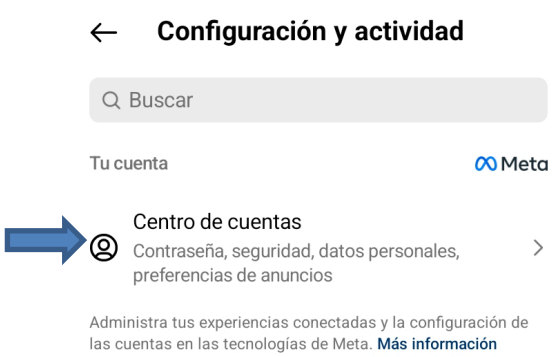


Imagen 2

⇒ Vaya a Contraseña y Seguridad. (Imagen 3)

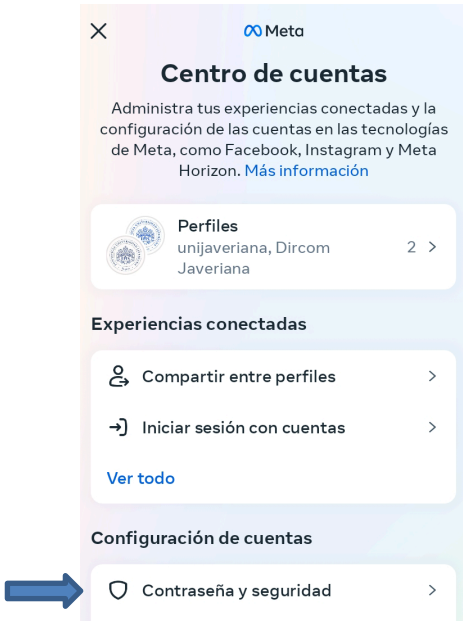


Imagen 3

Recuperar contraseña

Si olvidó la contraseña o perdió acceso a la cuenta, puede reestablecerla a través de alguno de los siguientes métodos:

⇒ Acceda a Instagram y dé clic en ¿Olvidaste tu contraseña? (en iOS) o ¿Has olvidado tus datos de inicio de sesión? (en Android), Obtén ayuda. (Imagen 4)

Imagen 4

⇒ Escriba su nombre de usuario o el correo asociado. A continuación, haga clic en *siguiente* y recibirá un correo electrónico con un enlace para cambiar la contraseña. (Imagen 5)

Imagen 5

⇒ Haga clic en dicho enlace, escriba una nueva contraseña y guarde los cambios. Si no recuerda el nombre de usuario o el correo, tendrá que utilizar otro método de ayuda.

⇒ Instagram permite acceder a la cuenta utilizando las credenciales de Facebook, la aplicación matriz. En la pantalla de inicio de sesión de Instagram, seleccione *¿Has olvidado tus datos de inicio de sesión?* (en Android) u *¿Olvidaste tu contraseña?* (en iOS). En la parte inferior de la pantalla haga clic en *Iniciar sesión con Facebook*. En iOS, esta opción también está disponible en la primera pantalla de inicio de sesión. Cuando Instagram solicite el permiso para iniciar sesión con Facebook, seleccione Continuar. (Imagen 6)

Imagen 6

⇒ Si sigue teniendo problemas para acceder a la cuenta, abra la aplicación de Instagram, escriba el nombre de usuario y dé clic en *Obtén ayuda*. Pulse el botón *Siguiente* y elija la opción *¿Necesitas más ayuda?* Siguiendo las instrucciones. (Imagen 7)

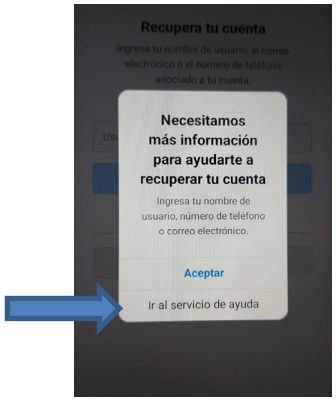


Imagen 7

Autenticación de dos factores

Para protegerse contra las filtraciones de contraseñas, active la autenticación en dos pasos. Siempre que alguien (incluido usted) intente iniciar sesión en

la cuenta desde un dispositivo diferente, la red social solicitará un código de un solo uso que recibirá mediante mensaje de texto o una aplicación especial. De esta forma, recibirá una notificación con todos los intentos de inicio de sesión, además, *hackear* la cuenta sin el código de un solo uso es mucho más complejo.

PARA ACTIVARLA:

⇒ Vaya al Centro de cuentas. (Imagen 8)

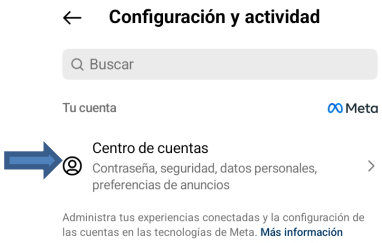


Imagen 8

⇒ Seleccione Contraseña y seguridad. (Imagen 9)

Imagen 9

⇒ Seleccione Autenticación en dos pasos. (Imagen 10)

Imagen 10

⇒ Seleccione cómo quiere recibir el código: mediante mensaje de texto o generado en una aplicación de autenticación (se recomienda el uso de Microsoft Authenticator y siga las instrucciones para cada caso. (Imagen 11)

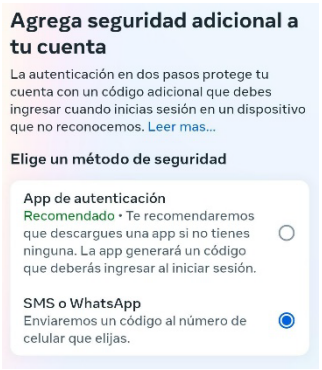


Imagen 11

Código de respaldo

Después de activar la autenticación de dos pasos la red social ofrece códigos de recuperación o respaldo. Estos códigos ayudan a iniciar sesión, aunque el celular asociado no esté a mano. Guarde los códigos en un lugar seguro.

Sesiones iniciadas

Además de tomar medidas para que otras personas no puedan acceder a la cuenta, también es útil revisar de vez en cuando si alguien entró. Para hacer esto, entre en el menú de *Centro de cuentas* desde el menú lateral al que puede acceder desde su perfil dentro de la aplicación.

⇒ Una vez dentro, pulse sobre la sección de Contraseña y seguridad. (Imagen 12)

Imagen 12

⇒ Elija la opción de Dónde iniciaste sesión. (Imagen 13)

Imagen 13

⇒ Esto abrirá una lista con los últimos inicios de sesión y su ubicación aproximada. Si detecta algún inicio de sesión sospechoso, podrá cerrarlo marcando No he sido yo.

Correos electrónicos de Instagram

Para evitar casos de *phishing* y comprobar que las notificaciones de la red social son auténticas:

⇒ Vaya a Centro de Cuentas, luego Contraseña y Seguridad. Después, seleccione Correos electrónicos recientes. (Imagen 14)

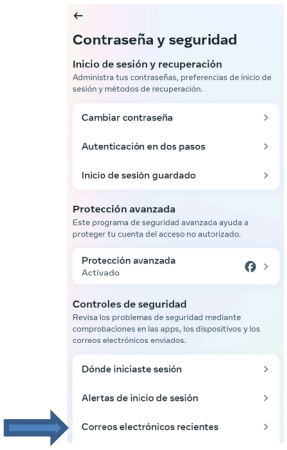


Imagen 14

Aquí aparecerán los correos electrónicos de Instagram de los últimos 14 días relacionados con seguridad e inicio de sesión. Se sugiere evitar al máximo usar aplicaciones de terceros, pues representan otra fuente de peligro.

Aplicaciones de terceros

Se sugiere evitar al máximo usar aplicaciones de terceros, pues representan otra fuente de peligro. Puede ver la lista de aplicaciones y sitios web conectados y eliminar los que no necesite en la sección *Seguridad*, en *Aplicaciones y sitios web*.

Filtro de Contenido

En caso de recibir comentarios injuriosos, ofensivos o que inciten a la violencia, se pueden borrar manteniendo el dedo pulsado sobre este para seleccionarlo, y dar clic en la opción de borrar.

⇒ Instagram tiene un filtro automático que detecta y oculta comentarios ofensivos. También se puede crear un filtro manual, añadiendo palabras no deseadas. Para hacerlo, entre en la Configuración, dé clic en la sección de Palabras Ocultas. (Imagen 15)

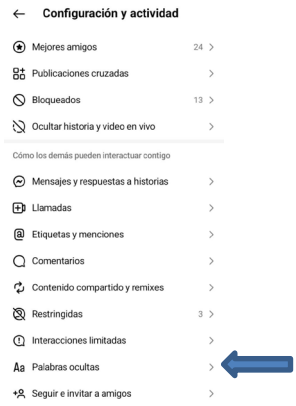


Imagen 14

Controles de seguridad automáticos

INTENTO DE *HACKEO*

Instagram ayuda a proteger las cuentas avisando a los usuarios cuando pudo haber un intento de *hackeo* e informando los pasos que debe seguir para protegerla: comprobar la actividad de inicio de sesión, revisar la información del perfil, confirmar las cuentas que comparten información de inicio de

sesión y actualizar la información de contacto para recuperar la cuenta, como su número de teléfono o su dirección de correo electrónico.

Para recuperar una cuenta *hackeada* siga las siguientes instrucciones: https://web.facebook.com/help/instagram/149494825257596?_rdc=1&_rdr

MENSAJES DIRECTOS

Instagram nunca enviará mensajes directos. Cuando se reciban mensajes de cuentas maliciosas solicitando datos confidenciales, contraseñas, etc., se recomienda reportar el contenido y bloquear la cuenta que envió el mensaje. Si alguna vez Instagram quiere ponerse en contacto con un usuario, lo hará a través de la opción Correos electrónicos de Instagram, mencionada anteriormente.

CUENTAS FALSAS

Instagram trabaja constantemente para detectar y detener las cuentas de personas que se hacen pasar por otras con el fin de *hackear*, atacar o engañar a los usuarios.

BUZÓN DE AYUDA

Para encontrar la información más reciente sobre la situación de los reportes o saber si alguna de las publicaciones infringe las políticas de Instagram, los usuarios puedes acceder al buzón de ayuda donde podrán ver con facilidad el estado de todo lo que se reportó o podrán apelar decisiones por posibles infracciones a las reglas de la red social.

⇒ Vaya a Configuración y actividad y deslice hasta la opción Estado de la cuenta (Imagen 16 y 17)

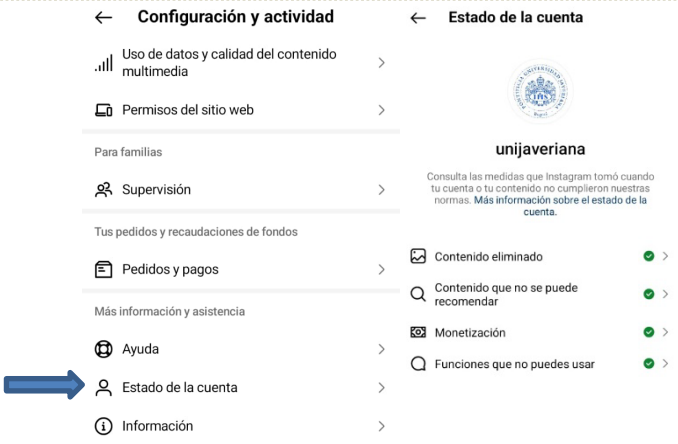
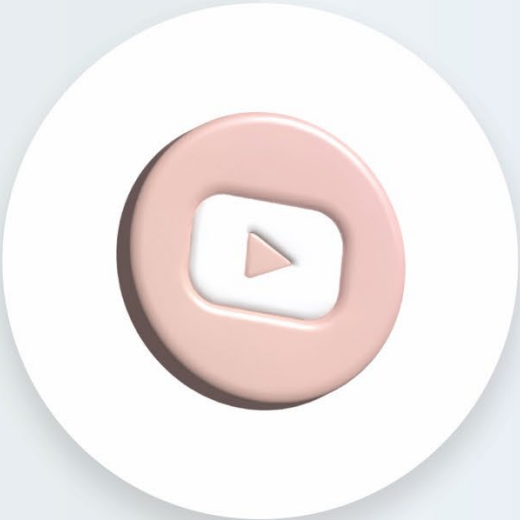


Imagen 16 - Imagen 17

5

YouTube



Capítulo V: YouTube

YouTube es la plataforma más popular para la publicación y visualización de videos. Los temas son variados: videos musicales, documentales, entretenimiento, piezas educativas, entre otras categorías.

Ajustes de Seguridad

Visite la página *Verificación de seguridad* para realizar tareas como agregar opciones de recuperación de la cuenta, configurar la verificación en dos pasos a fin de obtener mayor protección y consultar los permisos de la cuenta.

⇒ En YouTube, vaya a su cuenta de Google. (Imagen 1)

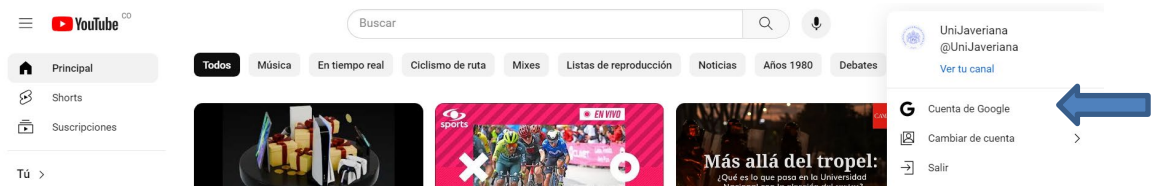


Imagen 1

Restablecer contraseña

La contraseña de YouTube es la misma que la de la cuenta de Google desde la cual se creó el canal (Debe ser una diferente a su cuenta personal). Para cambiar la contraseña de Google, siga los siguientes pasos:

⇒ Haga clic en seguridad. (Imagen 2)

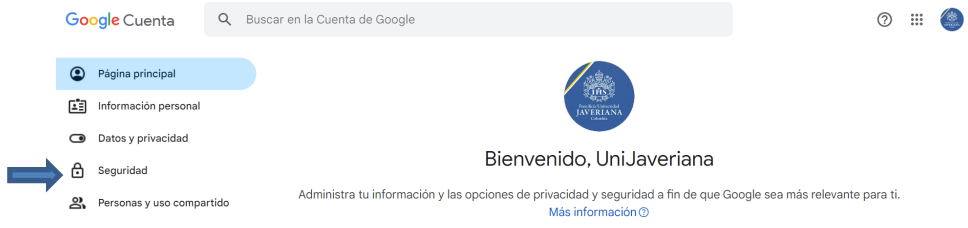


Imagen 2

⇒ Seleccione *Contraseña*. Es posible que deba volver a acceder. (Imagen 3)

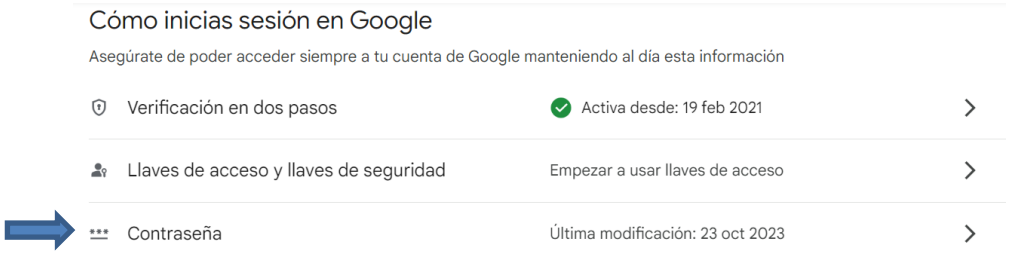


Imagen 3

⇒ Ingrese la contraseña nueva; luego, seleccione *Cambiar contraseña.* (Imagen 4)

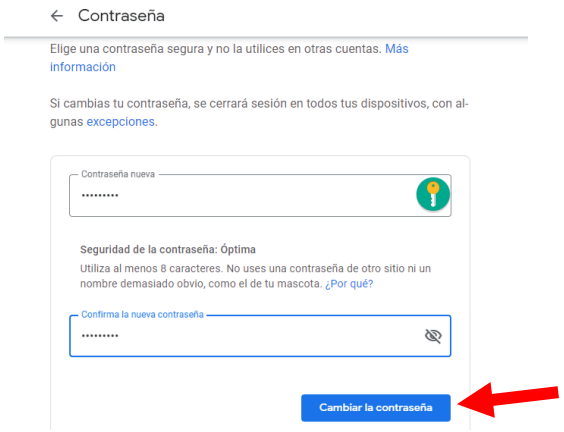


Imagen 4

Para reestablecer la contraseña de Google en caso de olvidarla o perder acceso a la cuenta:

⇒ Dé clic en *¿Olvidaste tu contraseña?* Google le enviará un mensaje de texto al número celular asociado o un mensaje al correo electrónico de respaldo. Es posible que Google le haga unas preguntas para verificar que es el propietario de la cuenta. (Imagen 5)

Imagen 5

Verificación en dos pasos

Agregue un número de celular de recuperación y un correo electrónico alternativo con dominio javeriana.edu.co a la cuenta de Google desde la cual se creó el canal de YouTube.

⇒ Vaya a la cuenta de Google desde la cual se creó el canal de YouTube. En Seguridad, vaya a Verificación en dos pasos y siga los pasos. (Imagen 6)

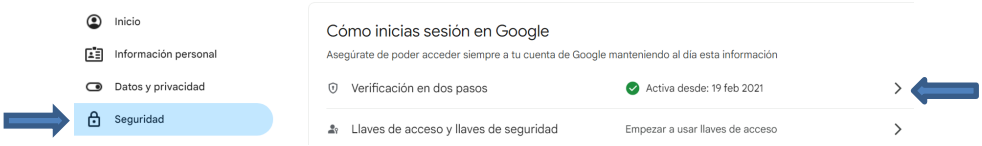


Imagen 6

CÓMO AGREGAR O CAMBIAR UN NÚMERO DE TELÉFONO DE RECUPERACIÓN

⇒ Vaya a la cuenta de Google desde la cual se creó el canal de YouTube. En el panel de navegación izquierdo, haga clic en *Información personal*. (Imagen 7)

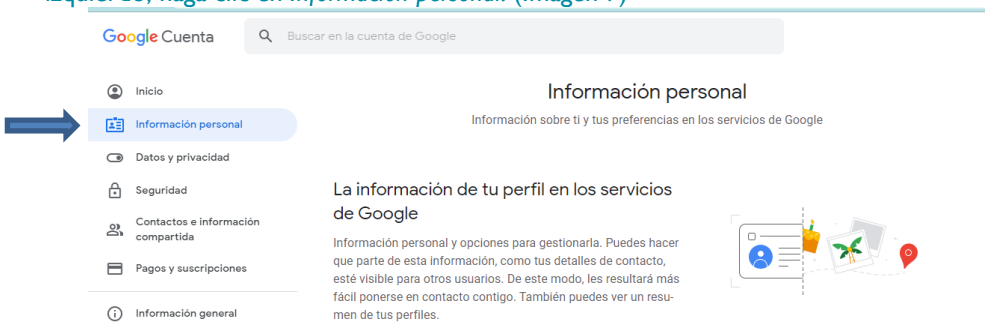


Imagen 7

⇒ En la sección Información de contacto, haga clic en Agregar un teléfono de recuperación para proteger la cuenta.

⇒ Agregue un número celular de recuperación.

⇒ Cambie el celular de recuperación: Junto al número, seleccione *Editar*.

⇒ Borre el teléfono de recuperación: Junto al número, seleccione *Borrar*.

⇒ Siga los pasos que aparecen en la pantalla.

⇒ Si borra el número de celular de recuperación, es posible que aún se use en otros servicios de Google. Vaya a la cuenta para administrar sus números de teléfono.

CÓMO AGREGAR O CAMBIAR UNA DIRECCIÓN DE CORREO DE RECUPERACIÓN

⇒ Vaya a la cuenta de Google desde la cual se creó el canal de YouTube.

⇒ En el panel de navegación izquierdo, haga clic en *Información personal*. (Imagen 7)

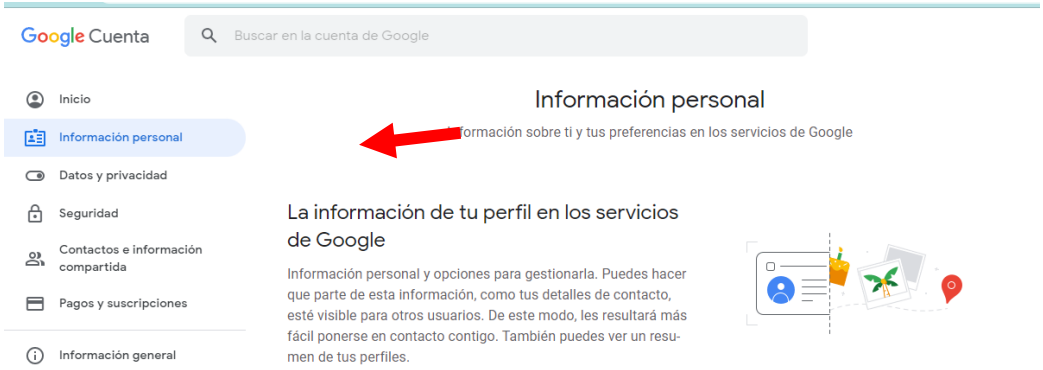


Imagen 7

⇒ En la sección Información de contacto, haga clic en *Correo electrónico*.

⇒ Agregue un correo de recuperación.

⇒ Cambie o borre el correo de recuperación: Junto al correo electrónico, seleccione *Editar*.

⇒ Siga los pasos que aparecen en la pantalla.

Aplicaciones de terceros

Se sugiere evitar al máximo usar aplicaciones de terceros. Estos sitios y aplicaciones tienen acceso a algunos datos de la cuenta de Google, incluida información que puede ser confidencial. Elimine el acceso para aquellos en los que ya no confía o no usa. Puede gestionarlos desde https://myaccount.google.com/permissions?hl=en

⇒ Vaya a Cuenta y Seguridad. (Imagen 8)

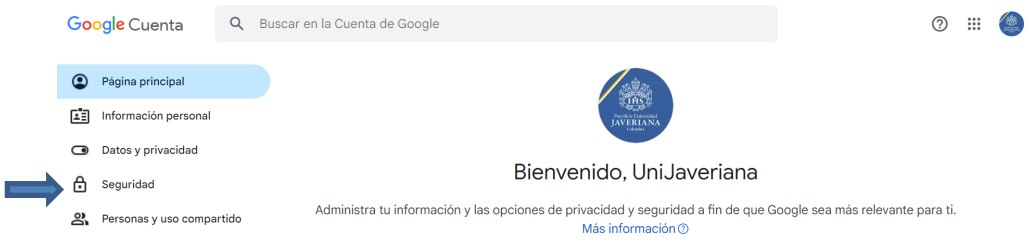


Imagen 8

⇒ Deslice hasta Tus conexiones con apps y servicios de terceros y haga clic en Ver todas las conexiones. Una vez allí, elimine aquellas aplicaciones que no corresponden a la gestión de esta cuenta. (Imagen 9)

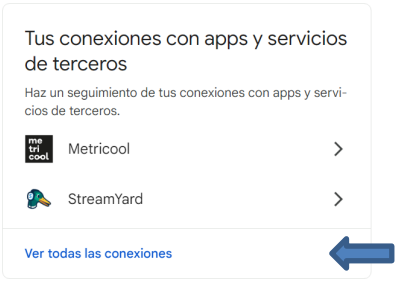


Imagen 9

NAVEGACIÓN SEGURA MEJORADA

Active la Navegación segura mejorada para obtener una protección más rápida y proactiva contra extensiones, descargas y sitios web peligrosos.

⇒ Vaya a su Cuenta, después seleccione Seguridad y deslice hasta la opción de Navegación Segura. Allí dé clic en Administra la Navegación segura mejorada y active esta opción. (Imagen 10)

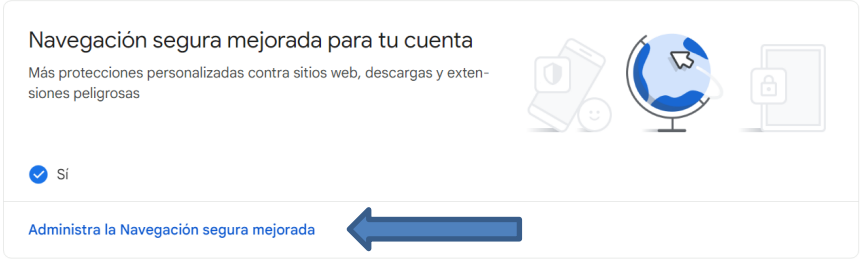


Imagen 10

Controles de seguridad automáticos

CENTRO DE AYUDA

YouTube cuenta con un centro de ayuda que puede visitar en https://support.google.com/youtube#topic=9257498 donde podrá encontrar recursos de privacidad y de seguridad, entre otros. (Imagen 11)

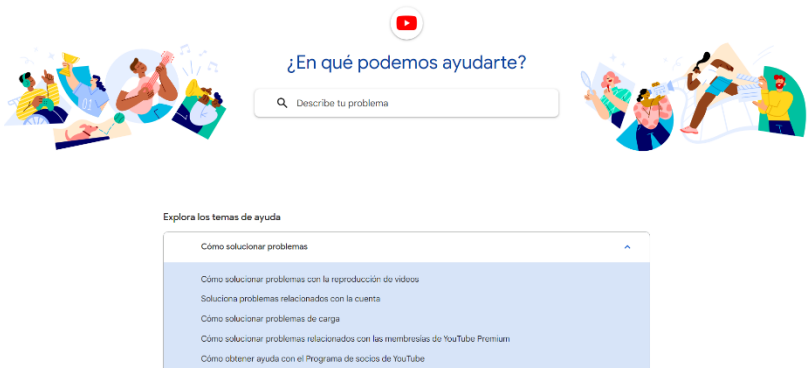


Imagen 11

POLÍTICAS SOBRE CUENTAS INACTIVAS

Si una cuenta permanece inactiva durante seis meses, es posible que YouTube elimine contenidos, sancione o cancele la cuenta sin previo aviso. También si la cuenta nunca ha subido un video, o si infringe los *Términos del Servicio* de YouTube o alienta a otros a infringirlos.

POLÍTICAS SOBRE SUPLANTACIÓN DE IDENTIDAD

En YouTube no se permite crear contenido para hacerse pasar por otra persona o canal. YouTube también obliga a que se respeten los derechos de

los titulares de marcas. Si considera que alguien suplantó el canal, siga estas instrucciones para denunciarlo:

https://support.google.com/youtube/answer/2802027#report_channel&zippy=%2Cc%C3%B3mo-denunciar-un-canal

CONTENIDO INAPROPIADO

Si desea denunciar contenido que considera inapropiado puede hacerlo de forma anónima a través de:

https://support.google.com/youtube/answer/2802027?hl=es

6

LinkedIn

LinkedIn es la mayor red de profesionales en el mundo, está orientada a generar relaciones comerciales y profesionales.

Ajustes de seguridad

La página *Configuración y privacidad* permite gestionar la configuración de privacidad y seguridad de la cuenta. Está organizada en seis secciones que ayudan a ver y modificar la información, las preferencias de privacidad, la configuración de anuncios y las notificaciones de comunicaciones.

Para acceder a esta página, siga estos pasos:

⇒ Haga clic en el icono de *Yo*, en la parte superior de la página de inicio. (Imagen 1)

Imagen 1

⇒ Seleccione *Ajustes y privacidad* en el menú desplegable. (Imagen 2)

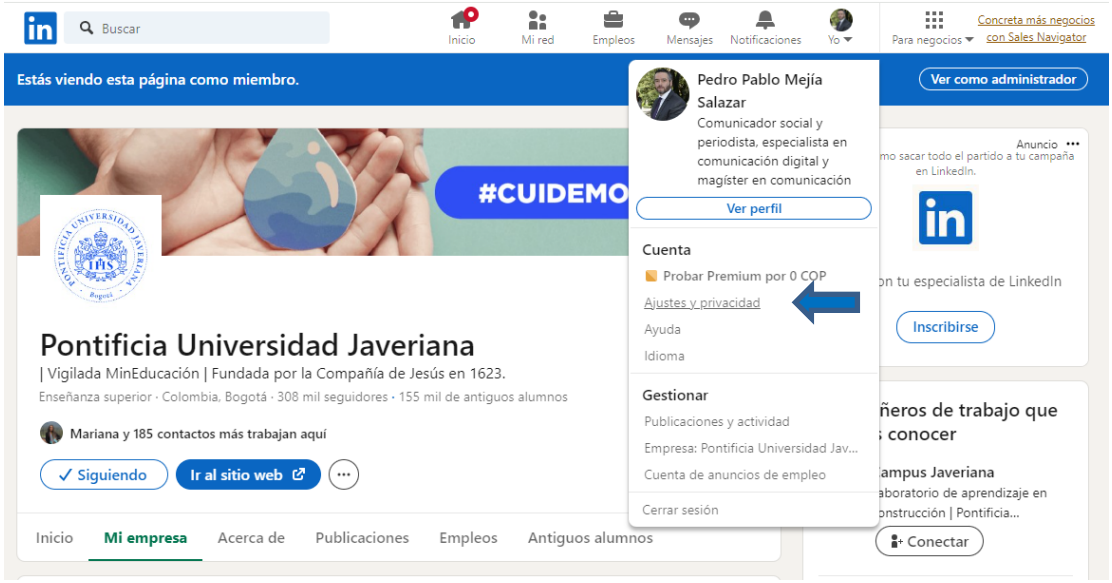


Imagen 2

Autenticación de dos factores

Seleccione una opción para el método de verificación de dos pasos que desee:

⇒ **Aplicación de autenticación**: este método utiliza un código de autenticación basado en una aplicación. Necesitará un teléfono que sea compatible con una aplicación de autenticación, como Microsoft Authenticator.

⇒ **Número de teléfono (SMS):** necesitará un teléfono que pueda recibir mensajes de texto SMS. El número de teléfono que introduzca en el proceso de verificación en dos etapas no aparecerá en la cuenta

CÓMO ACTIVAR O DESACTIVAR LA VERIFICACIÓN DE DOS FACTORES DESDE UN COMPUTADOR

⇒ Haga clic en *Inicio de sesión y seguridad* en el menú desplegable. (Imagen 3)

⇒ Haga clic en *Verificación en dos pasos.*

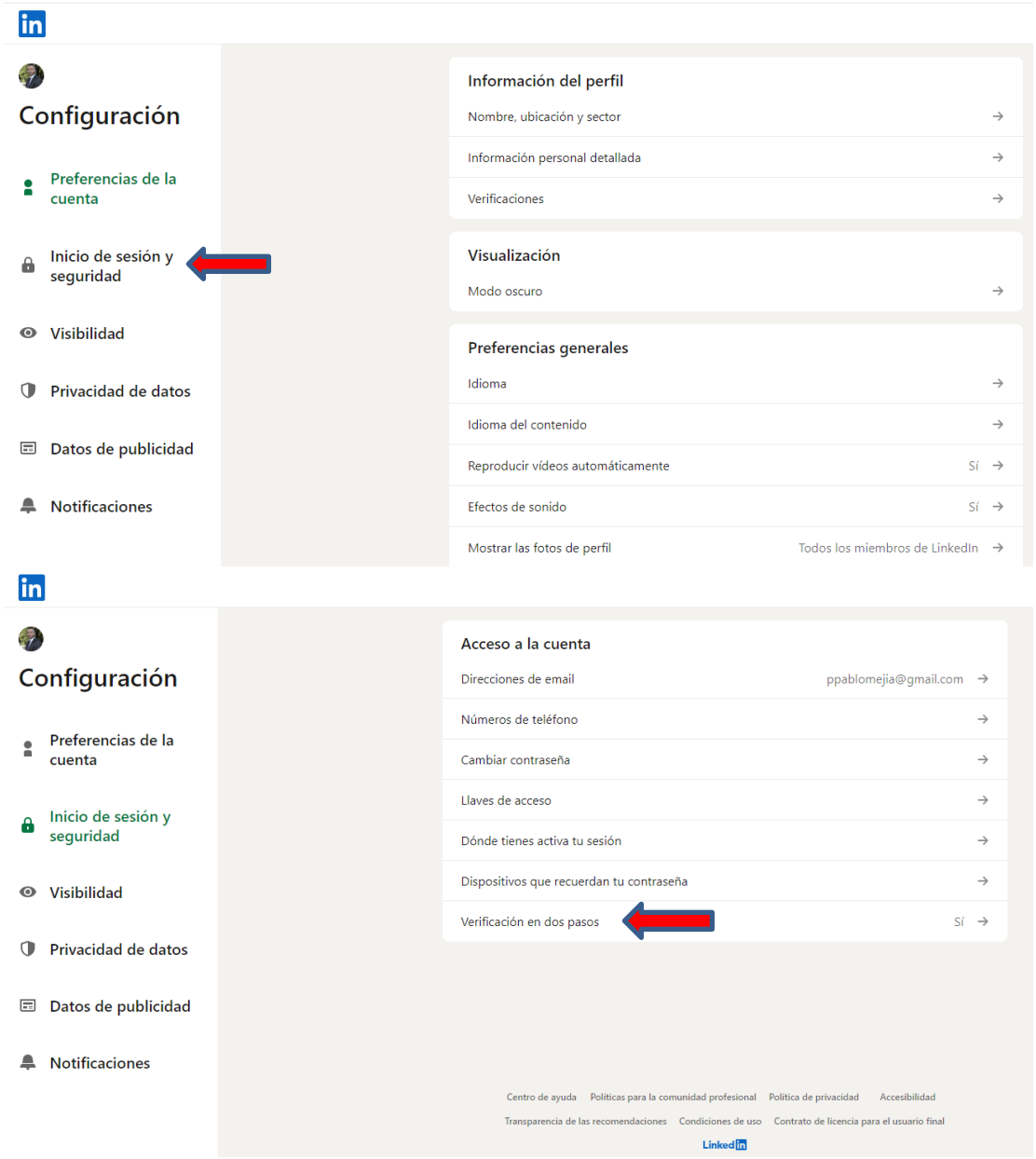


Imagen 3

⇒ Haga clic en *Activar* o *Desactivar* para cambiar el estado de la verificación en dos etapas.

⇒ Puede que se le pida que introduzca la contraseña por motivos de seguridad.

⇒ Seleccione el método de verificación preferido en la lista desplegable y haga clic en *Continuar*.

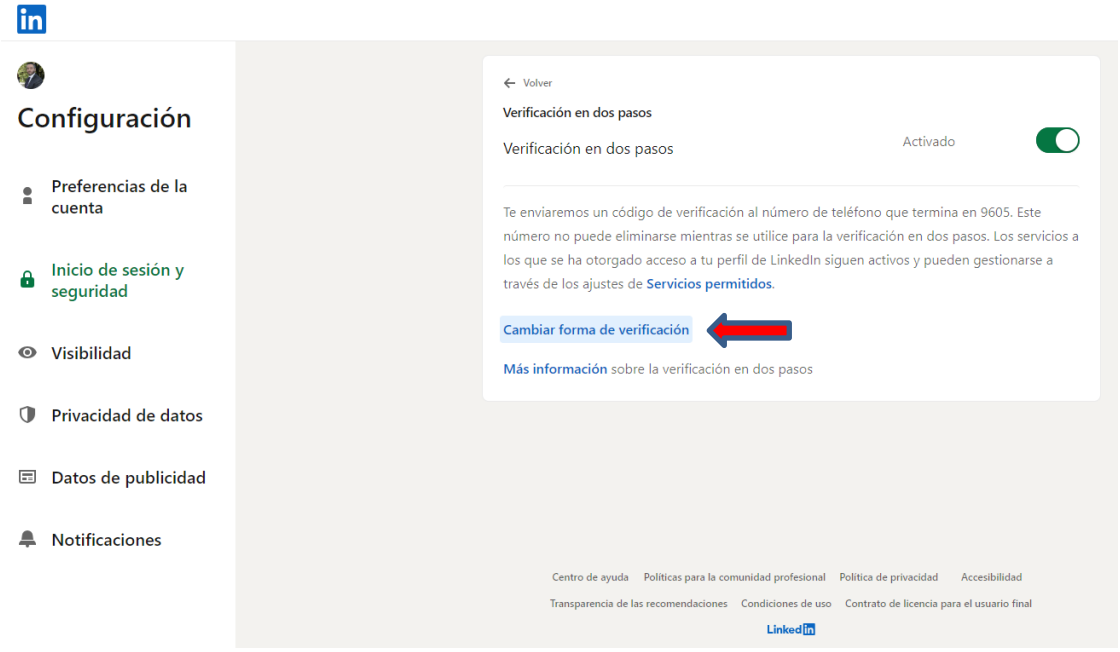


Imagen 4

CÓMO ACTIVAR O DESACTIVAR LA VERIFICACIÓN DE DOS FACTORES DESDE UN CELULAR:

⇒ Toque la foto de perfil, seleccione *Configuración*.

⇒ En Inicio de sesión y seguridad, y en Verificación en dos pasos. (Imagen 4 y 5)

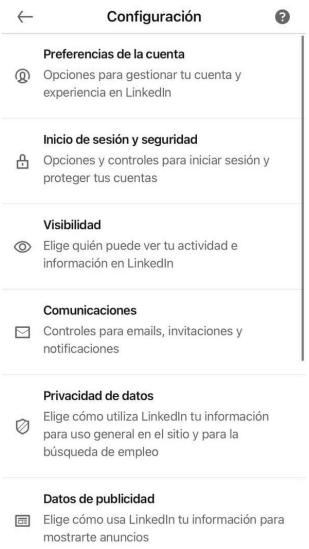


Imagen 4

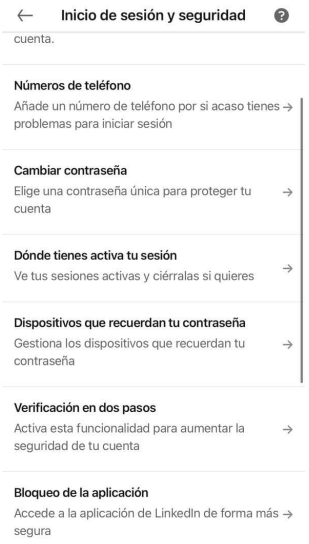


Imagen 5

⇒ Seleccione el método de verificación preferido en la lista desplegable y haga clic en *Continuar*.

⇒ Puede que se le pida que introduzca la contraseña por motivos de seguridad.

Roles de página

Asegúrese de familiarizarse con los diferentes roles de página que existen y los permisos que cada uno concede. Se recomienda revisar con regularidad quién tiene acceso de administrador en la configuración. Además, cuando agregue su página al administrador comercial, dedique un momento a conocer los permisos que otorga. También se recomienda que haya un administrador de contingencia en su página, de modo que, si alguna vez pierde acceso a ella, alguien de confianza pueda seguir manteniendo la página activa y agregarlo de nuevo.

Hay diez tipos de roles para quienes administran páginas. Cuando una persona crea una página, automáticamente se convierte en su administrador, lo que significa que puede cambiar su aspecto y publicar en su nombre. Solo los administradores pueden asignar roles y cambiar los roles de otras personas.

Tenga en cuenta que varias personas pueden tener roles en una página, pero cada una necesita su propia cuenta personal de LinkedIn.

En la siguiente tabla, se muestran los 10 roles de página y qué pueden hacer:

Súper Administrador	- Acceso a cualquier permiso de administrador - Añadir y eliminar administradores de la Página - Editar la información de la Página o desactivarla - Se pueden dar permisos totales a una persona o grupo de personas
Administrador de Contenido	- Crear y gestionar el contenido - Crear y gestionar las *stories* - Crear y gestionar eventos - Crear y gestionar ofertas de empleo
Curador de Contenido	- Publicar y tener acceso a todas las estadísticas de rendimiento del contenido
Analista	- Acceder a todas las analíticas de la página solo a través de la red social
Publicación de contenido pagado	- Crear anuncios con contenido patrocinado en nombre de la compañía - No se permite que publique directamente en la Página
Gestor de Leads	- Descargar los leads recibidos desde la Página
Creador de *Landing Pages*	- Crear *landing pages* asociadas con la Página de la empresa en LinkedIn
Anunciante de Contenido Patrocinado	- Crear anuncios de contenido patrocinado en nombre de la página desde una cuenta

		publicitaria de LinkedIn. Los anuncios no se muestran en el *feed* de la página
	Gestor de formularios de generación de contactos	- Descargar contactos desde la cuenta publicitaria de LinkedIn de la página
	Administrador de *Pipeline Builder*	- Permite crear páginas de destino centradas en la selección de personal y vinculadas a la página

CÓMO AÑADIR, EDITAR Y RETIRAR PERMISOS DE USUARIO EN LAS CUENTAS PUBLICITARIAS

Los administradores de medios de pago pueden crear contenido para la página con otras herramientas de LinkedIn, pero no tiene acceso a la vista de administrador.

CÓMO ACCEDER A LOS PERMISOS DE USUARIO DE UNA CUENTA PUBLICITARIA

⇒ Clique en *Configuración* y luego en *Gestionar administradores*

⇒ Clique en *Administradores de medios de pago* y luego en *Añadir administrador para medios de pago.*

⇒ Introduzca el nombre del usuario o la URL del perfil de LinkedIn

⇒ Seleccione una función de la lista desplegable

⇒ Clique en Guardar cambios

CÓMO EDITAR PERMISOS O ELIMINAR A UN ADMINISTRADOR

⇒ En *Configuración*, ingrese a la ventana emergente *Gestionar administradores, b*usque al usuario cuyos niveles de acceso quiere editar y haga clic en el ícono de lápiz (*Editar función de la página)* en la esquina superior derecha o en el ícono de caneca (*Eliminar como administrador de página*).

Controles de seguridad automáticos

LinkedIn no tolera actividades ni comportamientos inadecuados, como el correo no deseado, el acoso, el fraude y la información errónea. Sus políticas para la comunidad profesional indican las actividades aceptables e inaceptables y explican cómo denunciar spam y contenido abusivo o inapropiado. Ver el procedimiento en

https://www.linkedin.com/help/linkedin/answer/37822/recognizing-and-reporting-spam-inappropriate-and-abusive-content?src=direct%2Fnone&veh=direct%2Fnone%7Cdirect%2Fnone

CÓMO REPORTAR *PHISHING*

Si usted recibe un correo electrónico y cree que es un intento de *phishing*, por favor reenvíelo a phishing@linkedin.com. Si ve algún contenido sospechoso o que parezca ser fraudulento se recomienda denunciarlo haciendo clic en el ícono "…" que aparece en la parte superior derecha de la publicación. (Imagen 6)

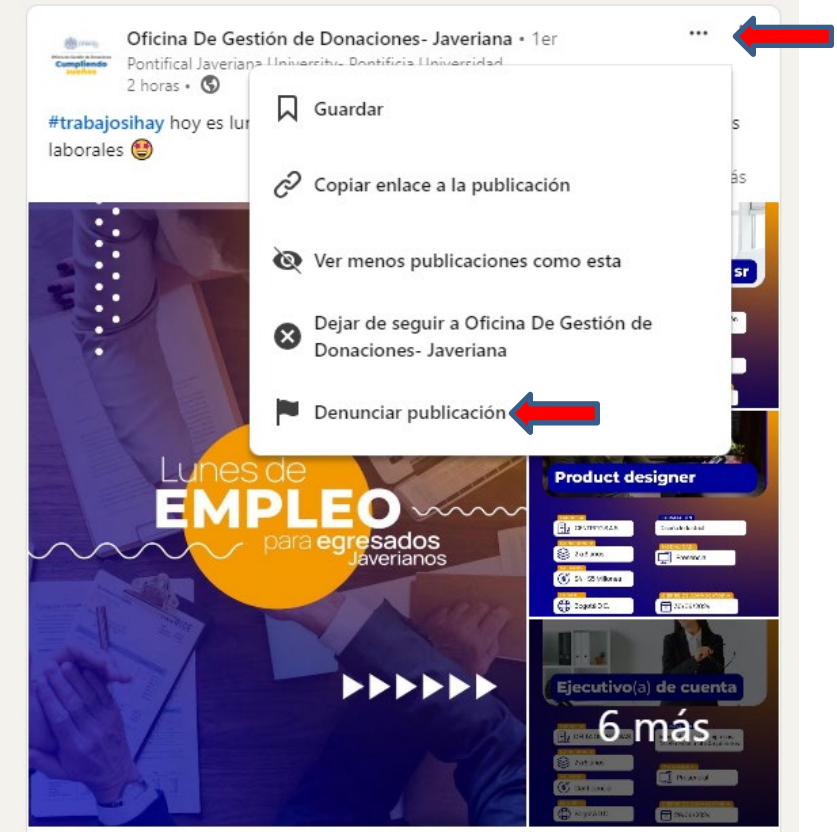


Imagen 6

FUSIONAR O CERRAR CUENTAS DUPLICADAS

Si recibe un mensaje que dice que la dirección de email que está intentando utilizar ya está en uso, es posible que tenga otra cuenta de LinkedIn con esa dirección de email. Sin embargo, antes de fusionar o cerrar una cuenta duplicada, tenga en cuenta otras razones por las que podría recibir este mensaje:

⇒ Utiliza varias direcciones de email diferentes.

⇒ Utiliza una dirección de email reciclada (una dirección que su empleador, o su proveedor de servicios de email, asignó a otra persona anteriormente).

⇒ Utiliza una dirección de email que incluye puntos u otros símbolos en la primera parte de la dirección, como a.bc@gmail.com.

Ver más información en:
https://www.linkedin.com/help/linkedin/answer/1275?src=direct%2Fnone&veh=direct%2Fnone%7Cdirect%2Fnone

DENUNCIAR INFORMACIÓN INEXACTA O PERFILES FALSOS

Si cree que un perfil puede ser falso, que es inapropiado o que contiene información falsa, puede denunciarlo dando clic en el ícono *Más* de dicha cuenta. Un perfil puede ser falso si aparece vacío o incluye palabras malsonantes, nombres falsos o se hace pasar por figuras públicas. (Imagen 7)

Imagen 7

LinkedIn actualiza periódicamente las Políticas para la comunidad profesional con el fin de asegurar que sus servicios sean libres de contenido o comportamientos no deseados o inapropiados.

Se recomienda consultar las Políticas para la comunidad profesional en https://es.linkedin.com/legal/professional-community-policies

7

TikTok

Capítulo VII: TikTok

TikTok es una popular plataforma de redes sociales que permite a los usuarios crear, compartir y descubrir videos cortos, generalmente acompañados de música de fondo. Con millones de usuarios activos en todo el mundo, TikTok ha ganado rápidamente popularidad, especialmente entre los jóvenes y adolescentes. Sin embargo, al ser una plataforma en línea, también presenta ciertos riesgos de seguridad que deben abordarse de manera proactiva.

Ajustes de seguridad

Para encontrar los ajustes de seguridad:

⇒ Abra el perfil.

⇒ Haga clic o pulse en las tres barras de la esquina superior derecha de la pantalla. (Imagen 1)

Imagen 1

⇒ Seleccione Ajustes y privacidad (Imagen 2)

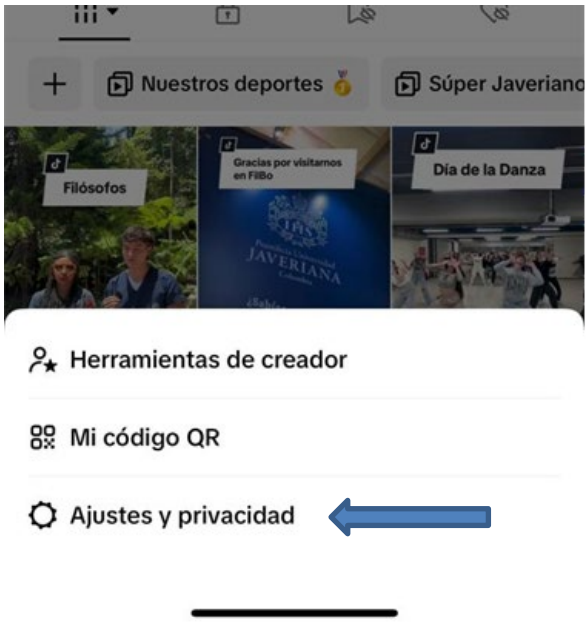


Imagen 2

⇒ Seleccione Seguridad y Permisos (Imagen 3)

Imagen 3

Restablecer contraseña

Si olvidó la contraseña o perdió acceso a la cuenta, puede reestablecerla a través de alguno de los siguientes métodos:

⇒ Abra TikTok y dé clic en *Usar teléfono, correo, usuario* (Imagen 4)

Imagen 4

⇒ Dé clic en *¿Olvidó contraseña?* (Imagen 5)

Imagen 5

⇒ Seleccione la manera para restablecer la contraseña (número de celular o correo), ingrese el número o el correo y siga los pasos que llegarán por mensaje de texto o a su correo electrónico registrado. (Imagen 6)


¿Olvidaste la contraseña?
Iniciar sesión
Restablece la contraseña con:
Número de teléfono
Correo electrónico
Cancelar

Imagen 6

Autenticación de dos factores

Habilite la autenticación de dos factores para agregar una capa adicional de seguridad a la cuenta. Esto requerirá un código de verificación adicional además de la contraseña al iniciar sesión en TikTok desde un nuevo dispositivo. Esto ocurrirá siempre que alguien (incluido usted) intente iniciar sesión en la cuenta desde un dispositivo diferente. De esta forma, recibirá una notificación con todos los intentos de inicio de sesión.

PARA ACTIVARLA:

⇒ Vaya a seguridad y permisos. (Imagen 7)

Imagen 7

⇒ Seleccione Verificación en dos pasos. (Imagen 8)

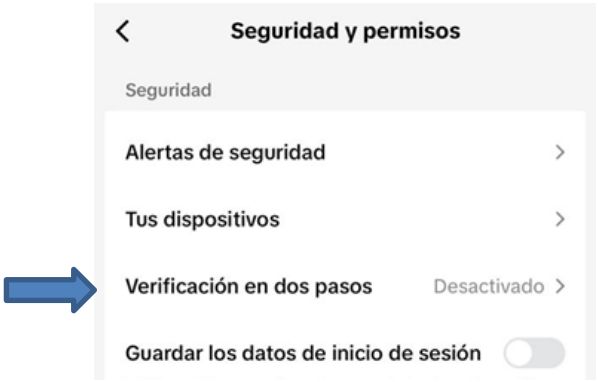


Imagen 8

⇒ Marque las dos opciones: mediante mensaje de texto o correo electrónico. (Imagen 9)

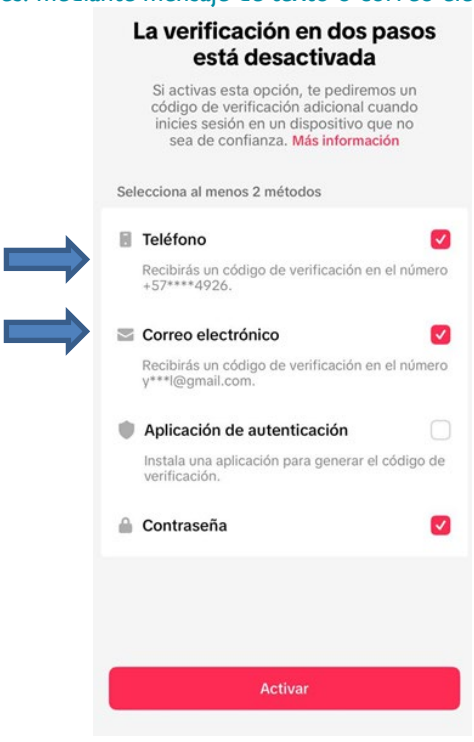
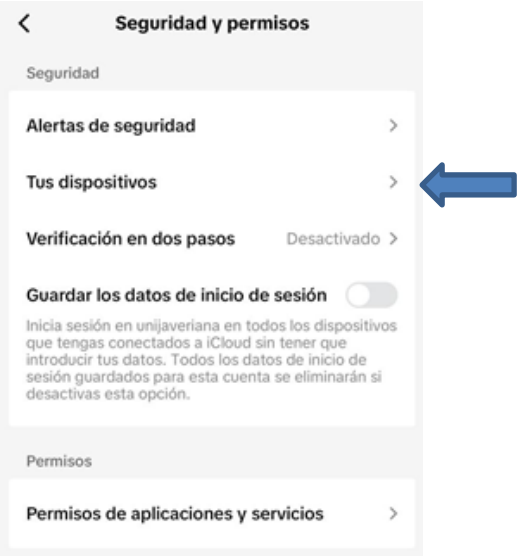


Imagen 9

Sesiones iniciadas

Revise regularmente las sesiones iniciadas en su cuenta para asegurarse que no haya sesiones activas en dispositivos desconocidos. Si detecta alguna actividad sospechosa, cierre la sesión en todos los dispositivos y cambie su contraseña de inmediato.

⇒ Para hacer esto, entre en el menú de seguridad y permisos desde el menú lateral al que puede acceder desde su perfil dentro de la aplicación. Una vez dentro, pulse sobre la sección de Tus dispositivos que verá en segundo lugar. (Imagen 10)



Esto abrirá una lista con los últimos inicios de sesión y su fecha. Si detecta algún inicio de sesión sospechoso, podrá cerrarlo dando clic en el ícono de eliminar.

Aplicaciones de terceros

Evite otorgar acceso a aplicaciones de terceros a su cuenta de TikTok, ya que esto podría comprometer la seguridad de su cuenta y sus datos personales. En caso de que sí, puede ver la lista de aplicaciones y sitios web conectados y eliminar los que no necesite en la sección Seguridad y permisos, en Permisos de aplicaciones y servicios.

Filtro de Contenido

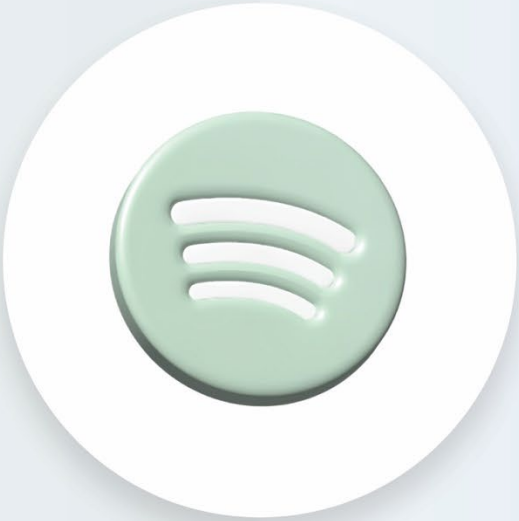
En caso de recibir comentarios injuriosos, ofensivos o que inciten a la violencia, se pueden borrar manteniendo el dedo pulsado sobre este para seleccionarlo, y dar clic en la opción de borrar.

Controles de seguridad automáticos

TikTok ofrece varias herramientas para controlar la seguridad y privacidad de las cuentas, que se pueden consultar en:
https://www.tiktok.com/safety/es-latam/safety-privacy-controls/

8

Spotify



Capítulo VIII: Spotify

Spotify es una plataforma de *streaming* para reproducción de música y *podcast*. Esta plataforma identifica tres tipos de usuarios: artistas, creadores de contenido (*podcasters*) y oyentes. En el ámbito institucional, Spotify permite subir *podcast* para divulgar contenido académico, cultural y de promoción institucional. También permite la creación de *playlist* musicales según las necesidades de las unidades.

Restablecer contraseña

Si olvidó la contraseña o perdió acceso a la cuenta, puede reestablecerla siguiendo estos pasos:

⇒ Ingrese a www.podcasters.spotify.com

⇒ Haga clic en *Iniciar Sesión* (Imagen 1)

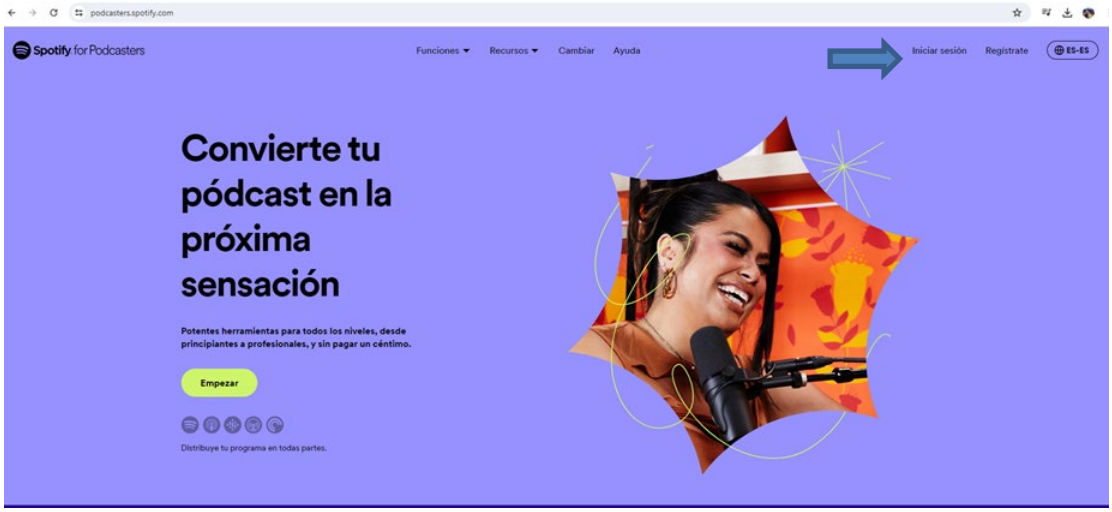


Imagen 1

⇒ Haga clic en ¿Se te ha olvidado la contraseña? (Imagen 2)

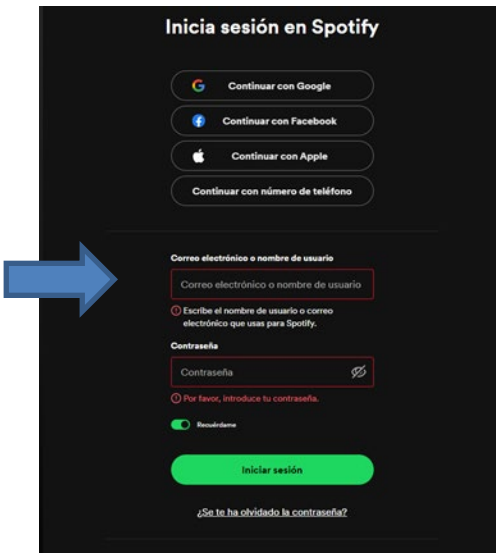


Imagen 2

Escriba el correo electrónico vinculado a la cuenta de Spotify y dé clic en enviar. Le llegará un mensaje al correo con el cual podrá cambiar la contraseña y recuperar la cuenta. (Imagen 3)

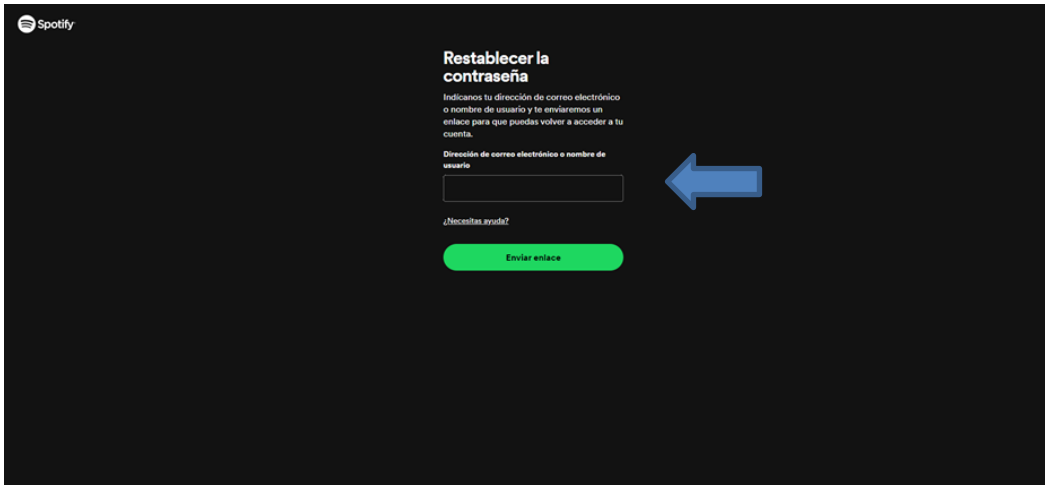


Imagen 3

⇒ Si no tiene acceso al correo dé clic en ¿Necesita más ayuda?, y lo comunicarán vía chat con un asesor. (Imagen 4)


Spotify
Restablecer la contraseña
Indícanos tu dirección de correo electrónico o nombre de usuario y te enviaremos un enlace para que puedas volver a acceder a tu cuenta.
Dirección de correo electrónico o nombre de usuario
¿Necesitas ayuda?
Enviar enlace

Imagen 4

Aplicaciones de terceros

⇒ Para subir contenido es necesario cargar previamente los archivos a una plataforma de alojamiento, vinculada a través de una fuente RSS a Spotify. Se recomienda que se use SoundCloud en su versión paga (esta tampoco debe estar asociada a Facebook, sino a un correo institucional), ya que permite controlar de forma manual en qué plataforma de *streaming* se va a publicar el contenido; esto también garantiza los derechos de autor del contenido de la Universidad y subir audios ilimitados sin riesgo de que se pierda información.

⇒ Se recomienda no vincular la cuenta de Spotify a Facebook, sino hacerlo directamente desde un correo institucional.

⇒ Si identifica un acceso no autorizado a su cuenta, se recomienda revocar el acceso a cualquier aplicación de terceros, ya que es posible que ese servicio también haya sido comprometido. Puede hacerlo a través del siguiente enlace: https://www.spotify.com/co/account/apps/?_ga=2.89234715.1077854968.1637782414-424557092.1616537644

Capítulo IX: Gestión de incidentes

¿Qué se considera un incidente?

Un evento indeseado o inesperado que pone en riesgo el acceso y la adecuada gestión de las redes sociales institucionales y que amenaza o afecta la reputación de la Pontificia Universidad Javeriana.

Categorización de incidentes:

La categorización de incidentes es un paso vital en el proceso de gestión de incidentes, pues permite que los eventos se prioricen y se atiendan oportunamente por los actores responsables. (Ver Responsables y Responsabilidades en la Introducción –página 10-)

- **Bajo:** Son aquellos eventos que no generan consecuencias significativas reputacionales o tecnológicas.
- **Medio:** Son aquellos eventos que no representan un alto peligro para la gestión de las redes sociales o para la reputación de la institución, pero que a mediano y largo plazo podrían agravarse de no ser atendidos oportunamente.
- **Alto:** Son aquellos eventos que representan un alto peligro para la gestión de las redes sociales o para la reputación de la institución si no son atendidos de inmediato.
- **Extremo:** Son aquellos eventos que ya generaron la pérdida de acceso a las redes sociales o una afectación grave de la reputación institucional y su atención debe ser inmediata.

Proceso para la atención de incidentes

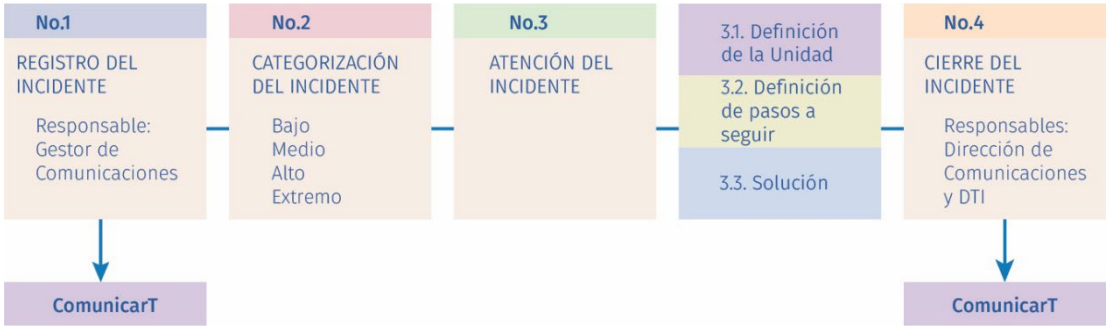
Se activa una vez un gestor de comunicación identifique un posible incidente de seguridad en las redes sociales que administra. Inmediatamente detecte el problema deberá seguir el siguiente proceso:

1. **Registro:** Lo reporta a la Dirección de Comunicaciones a través de ComunicarT* en la categoría ***"Incidentes de seguridad en redes sociales"*** diligenciando la siguiente información:
    - Nombre del usuario
    - Email
    - Unidad
    - Número de contacto
    - Cargo
    - Jefe inmediato
    - Red social afectada
    - Descripción detallada del incidente
    - Fecha y hora del incidente
    - Acciones realizadas para resolver el incidente

- Atención requerida
- Evidencia (Enlace o captura de pantalla)

2. **Categorización:** La Dirección de Comunicaciones categoriza el evento reportado para definir con qué urgencia debe solucionarse.
3. **Solución**:
    a. Definir la(s) unidad(es) que debe(n) atender el incidente
        i. Si el incidente puede ser solucionado por el mismo gestor, la Dirección de Comunicaciones le orientará para solucionarlo.
        ii. Si el incidente puede ser solucionado por la Dirección de Comunicaciones, esta lo atenderá de forma oportuna.
        iii. Si el incidente requiere soporte avanzado se escalará a la DTI para su solución.
        iv. Si el incidente genera una crisis institucional se le reportará al Comité de Crisis.
    b. La(s) unidad(es) encargada(s) se reunirán para determinar cuáles serán los pasos que se deben seguir para solucionar el incidente.
    c. Se aplica la solución.
4. **Cierre:** La Dirección de Comunicaciones, con el apoyo de la DTI, y de la unidad involucrada, documentará el incidente a través de la respuesta y cierre del caso en ComunicarT, incluyendo las posibles causas del incidente, las acciones que se realizaron para atenderlo y las recomendaciones que se deben seguir para evitar que se repita.

Flujograma de actividades



Glosario

Glosario

Adware: Es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador. Puede ser un precursor de los PUP (programas potencialmente no deseados). Normalmente, recurre a un método oculto: bien se hace pasar por legítimo para engañarlo e instalarse en su PC, tableta o celular. (https://es.malwarebytes.com/adware/)

Android: Es un sistema operativo que fue creado especialmente para teléfonos con pantalla táctil, los llamados de nueva generación o los inteligentes, las tabletas comunes y las que funcionan con líneas telefónicas; entrando en esta gama los relojes inteligentes, televisores y algunos aditamentos de los nuevos automóviles. (https://conceptodefinicion.de/android/)

App Store: Es la plataforma de descarga de aplicaciones móviles o apps de los dispositivos con sistema operativo iOS y Mac Os de la empresa Apple. A través de ella los usuarios pueden descargar aplicaciones de todo tipo, juegos, libros, redes sociales, películas, música y demás contenido. (https://www.arimetrics.com/glosario-digital/app-store)

App de autenticación: Es una aplicación de seguridad móvil que genera códigos de seguridad para iniciar sesión. Los más comunes en las *Stores* de Android y Apple son: Google Authenticator, Microsoft Authenticator, Authy, Lastpass Authenticator, entre otros.

Bluetooth: Es una tecnología de red que sirve para la transmisión inalámbrica de datos (fotos, música, contactos…) y voz entre diferentes dispositivos que se hallan a corta distancia, dentro de un radio de alcance que, generalmente, es de diez metros. Por ejemplo, gracias a esta tecnología, podemos vincular nuestro celular con una impresora para imprimir nuestras fotos preferidas sin necesidad de cables. (https://www.ionos.es/digitalguide/servidores/know-how/que-es-bluetooth/)

Certificado de seguridad SSL: Es un pequeño archivo de datos que vincula digitalmente una clave criptográfica con los datos de una organización. Una vez instalado en el servidor web, el certificado activa el candado y el protocolo https y, de esta forma, se habilita una conexión segura desde el servidor web hasta el navegador. (https://www.globalsign.com/es/ssl-information-center/what-is-an-ssl-certificate)

Código QR: 'Códigos de respuesta rápida' (definición del original en inglés *Quick Response code*), códigos de barras bidimensionales que almacenan datos codificados que pueden ser leídos o descargados desde dispositivos móviles.

Cookies: En el contexto de la tecnología, una *cookie* es un archivo que envía un sitio web y que se almacena en el navegador de la persona que está usando Internet. Este archivo permite que el sitio rastree la actividad que se realiza en el navegador. Al aceptar las cookies (mensaje de advertencia obligatorio) el usuario autoriza que el sitio rastree datos como la ubicación, hábitos de navegación y otra información asociada. (https://definicion.de/cookie/)

Cortafuegos (Firewalls): Es un dispositivo de seguridad que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza. Un *firewall* puede ser *hardware*, *software* o ambos. (https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html)

Dirección IP: Es un número que permite la identificación de una interfaz en red de una computadora (ordenador), un teléfono inteligente u otro dispositivo que usa el mencionado protocolo. Esta dirección puede ser estática o dinámica. (https://definicion.de/direccion-ip/)

Encriptar: Técnica con la cual el mensaje es protegido de la lectura de terceros. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito. Las últimas generaciones de navegadores, como Netscape Navigator 2.0, incluyen sistemas automáticos de encriptación. (https://sistemas.com/encriptar.php)

Fuente RSS: Es un formato XML que sirve para distribuir contenido a través de Internet, actualizándose de una forma automatizada y con una fuente única para quien distribuye la información. Es como una especie de "cédula" para poder distribuir la información

Hacker: Persona que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo. Los hackers también son conocidos como "piratas informáticos". (https://www.significados.com/hacker/)

IOS: Es el sistema operativo diseñado por Apple para sus productos, iPhone, iPad, iPod Touch, y Apple TV. Otros dispositivos como el iPod Nano y el iWatch utilizan otro sistema más básico y dirigido a una función más específica basado en iOS porque incorpora algunos de sus gestos e iconos y además se pueden sincronizar con teléfonos o tabletas. (https://conceptodefinicion.de/ios/)

Feed: Es la página de inicio de una red social, es un conglomerado de información relacionado directamente con la red de contactos y los intereses del usuario.

Malware: Es un término genérico utilizado para describir una variedad de *software* hostil: virus informáticos, gusanos, caballos de Troya, *software* de rescate, *spyware*, *adware*, *software* de miedo, etc. También puede encriptar o eliminar datos confidenciales, modificar o desviar las funciones básicas del ordenador, espiar la actividad informática de los usuarios. Lo usan los ciberdelincuentes para ganar dinero, pero también puede usarse con fines de sabotaje por razones políticas. (https://www.oracle.com/es/database/security/que-es-el-malware.html)

Man-in-the-Middle: Un criminal cibernético o software malicioso que se incrusta entre la víctima y la fuente de datos (cuentas bancarias, email, etc.). El objetivo es interceptar, leer o manipular el acceso de la víctima a sus datos sin que nadie se dé cuenta de que hay un tercero en la operación. (https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/)

Método OAuth de X: Es un protocolo abierto que permite la autorización segura en un método simple desde aplicaciones web, móviles y de escritorio. OAuth es el marco de autorización más común hoy en día, y se utiliza en la mayoría de las aplicaciones y servicios web comunes, como GitHub, Google, Facebook y, por supuesto, X. (https://code.tutsplus.com/es/tutorials/how-to-authenticate-users-with-twitter-oauth-20--cms-25713)

Landing Page: Es una página web preliminar o página de aterrizaje que sirve para destacar algo en especial, ya sea un producto, o alguna novedad o promoción de un producto. (https://www.mdmarketingdigital.com/blog/que-es-una-landing-page-y-para-que-sirve/)

Leads: Es una persona o compañía que ha demostrado interés en la oferta de la marca, mostrando dicho interés a través de una solicitud o de la oferta de sus datos a través de un canal puede ser una página de Facebook, X, LinkedIn o una página web entre otros. Estos contactos pasan a formar parte de una base de datos y son considerados clientes potenciales de productos o servicios. (https://www.cyberclick.es/lead)

Navegadores de incógnito: El modo privado o el modo incógnito es una función de privacidad en algunos navegadores web para desactivar el historial de navegación y la caché web. Esto permite a una persona navegar por la web sin almacenar datos locales en el historial del navegador y que podrían ser recuperados más tarde. No es lo mismo navegación privada que navegación anónima, ya que existen diferencias entre ambos conceptos. (https://www.arimetrics.com/glosario-digital/navegacion-privada)

Newsfeed: El *feed* web es el sistema principal a través del cual los usuarios están expuestos al contenido publicado en una red social. News Feed destaca información que incluye cambios de perfil, próximos eventos

y cumpleaños, entre otras actualizaciones. Es una característica de Facebook.(https://en.wikipedia.org/wiki/News_Feed)

NFC (Near Field Communication): Es una sigla que alude a la expresión inglesa *Near field communication*, que puede traducirse al castellano como "Comunicación de campo cercano". Así se denomina a una tecnología de comunicación sin cables (inalámbrica). La tecnología NFC se utiliza para intercambiar datos entre teléfonos celulares u otros dispositivos. El NFC posibilita la lectura-escritura en ambos sentidos. Esto quiere decir que los dispositivos pueden emitir y recibir señales de manera simultánea. (https://definicion.de/nfc/)

Notificación push: Es un mensaje corto en una aplicación o basado en la web. Las notificaciones push se utilizan para diversos fines: desde el envío de mensajes del sistema y actualizaciones de la aplicación hasta promociones. Se usa para dar más valor y mantener a los usuarios comprometidos con la marca.
(https://sendpulse.com/latam/support/glossary/push-notification)

Phishing: Es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundir miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia como bloqueo de cuentas.
(https://es.malwarebytes.com/phishing/)

Pipeline Builder: Es una herramienta que proporciona LinkedIn a través de una inversión mínima en anuncios y que tiene una duración anual, es decir, se puede utilizar como página de destino de varias campañas y modificar la información a lo largo de todo el año que está activa.
(https://www.wtcspain.eu/blog/linkedin-pipeline-builder-alcanzar-y-contratar-el-talento-de-calidad/#:~:text=Pipeline%20Builder%20es%20una%20herramienta,el%20a%C3%B1o%20que%20est%C3%A1%20activa)

Playlist (Lista de reproducción): Una lista de reproducción de archivos de video o audio que se pueden reproducir en un reproductor multimedia de forma secuencial o en orden aleatorio.
(https://en.wikipedia.org/wiki/Playlist)

Podcast: Un podcast es una publicación de carácter digital y periódica, en formato de audio que se puede descargar de Internet o escuchar online. Es

un archivo de audio personalizable y descargable que puede montarse en una página web, en un blog o en todo tipo de plataformas para que esté a disposición de los usuarios y/o seguidores. (https://www.elespanol.com/como/podcast-definicion-funcionamiento/461204772_0.html)

Protocolo https: Es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. (https://developers.google.com/search/docs/advanced/security/https?hl=es)

Software: Según la RAE, el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. Abarca todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo, los editores de imágenes, los reproductores de audio y los videojuegos, entre otras muchas. (https://definicion.de/software/)

Spam: Es la denominación del correo electrónico no solicitado que recibe una persona. Dichos mensajes, también llamados correo no deseado o correo basura, suelen ser publicidades de toda clase de productos y servicios. Suelen llegar de forma masiva e insistente. (https://definicion.de/spam/)

Spyware: Es cualquier componente de software malicioso que infecta su ordenador y espía sus datos personales. Estos programas pueden robar información personal como búsquedas e historiales, usuarios y contraseñas, y detalles de la tarjeta de crédito. (https://softwarelab.org/es/que-es-spyware/)

Streaming: Es un tipo de tecnología multimedia que envía contenidos de vídeo y audio a un dispositivo conectado a Internet. Esto le permite acceder a videos, películas, música, podcast en cualquier momento que lo desee, desde un computador o celular. (https://www.avast.com/es-es/c-what-is-streaming#gref)

TOTP: Sus siglas indican, *Time-Based One-Time Password*. Es una contraseña válida solo durante un breve periodo después. El Grupo de trabajo de ingeniería de internet (IETF) publicó en 2011 el algoritmo *Time-based One-time Password* en el RFC 6238 para proporcionar una mayor seguridad en Internet.

Estas contraseñas únicas son especialmente populares como parte de una autentificación multifactor. Para ello, en el inicio de sesión en un servicio web los usuarios utilizan en primer lugar su contraseña personal fija y, de manera adicional, se genera una contraseña especial para ese proceso de inicio de sesión durante un periodo limitado. El usuario la recibe, p. ej. a través de una aplicación o de un dispositivo especial (token).

Si la contraseña se usa una vez o no durante un tiempo, caduca. Por lo tanto, para los criminales es muy complicado acceder al segundo factor. Incluso aunque conozcan la contraseña, tendrán muy pocas posibilidades de solicitar también el TOTP o no dispondrán del tiempo suficiente para descifrarlo.

. (https://www.ionos.es/digitalguide/servidores/seguridad/totp/)

Troubleshooting: es una forma de resolución de problemas, a menudo aplicada para reparar los productos o procesos fallidos. Es una búsqueda lógica y sistemática de la fuente de un problema para que pueda ser resuelto, por lo que el producto o proceso puede volver a funcionar. La solución de problemas se utiliza en muchos campos, como ingeniería, administración de sistemas, electrónica, reparación de automóviles y medicina de diagnóstico. (https://educalingo.com/es/dic-en/troubleshooting)

URL: Es una sigla correspondiente a *Uniform Resource Locator* (Localizador Uniforme de Recursos). Se trata de la secuencia de caracteres que permite ubicar recursos en Internet para que puedan ser localizados. Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen una URL cuando se publican en Internet. Estos localizadores permiten crear hipervínculos (también conocidos como enlaces o links) en la World Wide Web (WWW), lo que facilita la navegación.

Virtual private network (VPN): Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían.

Pontificia Universidad
JAVERIANA
Colombia