Redes sociales

Capítulo destinado a la configuración de seguridad y ajustes de privacidad en redes sociales.

- Ajustes de seguridad y privacidad en redes sociales
- Gestión segura de cuentas y páginas de redes sociales

Ajustes de seguridad y privacidad en redes sociales

Twitter

- Habilitar la protección de restablecimiento de contraseña https://twitter.com/settings/security
- Habilitar la autenticación en dos fases: https://twitter.com/settings/security
- Revisar los últimos inicios de sesión regularmente https://twitter.com/settings/applications

Facebook

- Habilitar alertas sobre inicios de sesión no reconocidos: https://www.facebook.com/settings?tab=security
- Habilitar la autenticación en dos pasos: https://www.facebook.com/security/2fac/settings/
- Elegir contactos de confianza para recuperar acceso a la cuenta:
  - https://www.facebook.com/settings/?tab=security§ion=trusted_friends&view
- Revisar los Inicios de sesión autorizados regularmente: https://www.facebook.com/settings/?tab=security&view

Instagram

- Habilitar la autenticación en dos pasos. En la aplicación móvil: Configuración > seguridad > autenticación en dos pasos > habilitar APP
- Revisar la lista de aplicaciones y sitios web conectados. Eliminar los que no son necesarios. En la aplicación móvil: Configuración > Seguridad, > Aplicaciones y sitios web.
- Revisar la actividad de inicio de sesión regularmente. En la aplicación: Configuración > seguridad > seguridad de inicio de sesión.

Servicios de Google (YouTube, Gmail, etc)

- Revisar el estado de la seguridad regularmente https://myaccount.google.com/security-checkup

- Habilitar la autenticación en dos pasos: https://myaccount.google.com/signinoptions/two-step-verification
- Revisar la lista de aplicaciones y sitios web conectados: https://myaccount.google.com/permissions
- Configurar un correo de recuperación de cuentas: https://myaccount.google.com/recovery/email?edit
- Configurar un teléfono de recuperación de cuentas: https://myaccount.google.com/signinoptions/rescuephone?edit

En general

- Usar un contenedor de contraseñas como https://keepass.info/ para generar y almacenar las contraseñas.
- No reutilizar la contraseña en otros sitios web.
- Asegurar que el software en el equipo, incluido el navegador, esté al día con las últimas actualizaciones.

Gestión segura de cuentas y páginas de redes sociales

1. Introducción

La interacción entre las organizaciones públicas y privadas con la sociedad ha experimentado un notable aumento gracias a la adopción de plataformas tecnológicas, las cuales van más allá de los métodos tradicionales como formularios de contacto, correo electrónico o teléfono. Nos referimos principalmente a las Redes Sociales, las cuales, dentro de su diversidad, presentan algunas opciones más populares que otras debido a factores como funcionalidad y cantidad de usuarios.

Esta creciente popularidad ha convertido a estas plataformas en blanco de ataques por parte de individuos que aprovechan cualquier posible fallo en las aplicaciones para acceder a cuentas de usuarios, dependiendo del grado de criticidad de la vulnerabilidad. Asimismo, existen debilidades por parte de los usuarios, como una gestión deficiente de sus cuentas, como por ejemplo, contraseñas poco complejas.

Por lo tanto, resulta fundamental adoptar prácticas de seguridad en la administración de las cuentas de redes sociales para minimizar la ocurrencia de incidentes. Aunque las plataformas implementan esfuerzos para proteger a sus usuarios mediante la incorporación de mecanismos de seguridad, es importante reconocer que no existe un sistema completamente seguro.

Además, los incidentes de seguridad también pueden ser causados por acciones del propio usuario, ya que los atacantes suelen aprovecharse de las malas prácticas de seguridad mediante técnicas de ingeniería social, el engaño, así como la sobre exposición de información personal y otros datos públicos.

2. Amenazas

Las amenazas son potenciales peligros o riesgos que podrían comprometer la seguridad de los datos. Estas pueden provenir de actores de amenaza que utilizan tácticas y técnicas para poder obtener información sensible o confidencial como ser una fecha de nacimiento, números de tarjetas de débito o una contraseña. A continuación se enumeran a los actores de amenaza y las tácticas y técnicas que utilizan.

2.1. Actores de amenaza

2.1.1. Hacktivistas

Los hacktivistas son individuos o grupos que utilizan sus habilidades técnicas en actividades de hackeo para promover causas políticas, sociales o ideológicas. Su objetivo principal es influir en la opinión pública, llamar la atención sobre problemas sociales o políticos, o protestar contra organizaciones, gobiernos o empresas mediante acciones cibernéticas.

Los hacktivistas realizan ataques informáticos, para poder obtener una contraseña que les permita acceder a una cuenta y desde la misma realizar sus campañas de activismo político, social o ideológico.

2.1.2. Cibercriminales

Los cibercriminales son individuos o grupos que se dedican a actividades delictivas en línea con fines económicos, financieros o personales. Su objetivo principal es obtener beneficios financiero o causar daño mediante actividades como el robo, secuestro y divulgación de información confidencial, la propagación de malware, el secuestro de datos, el robo de identidad, entre otros. Los cibercriminales suelen actuar de manera encubierta y están motivados por el lucro personal o la ganancia económica ilícita al vender las contraseñas o realizar ataques aprovechando el acceso no autorizado a las cuentas comprometidas.

2.1.3. Personal descontento

El personal puede tener acceso a información confidencial o a sistemas críticos debido a sus roles y responsabilidades dentro de la entidad. Si existe personal descontento o desvinculado, estos podrían aprovechar su nivel de acceso a la información o tratar de obtenerla aprovechando el descuido del personal que no resguarda adecuadamente sus credenciales y el acceso a sus dispositivos.

2.2. Técnicas y tácticas

2.2.1. Phishing

El phishing es una técnica utilizada para engañar a las personas y obtener información confidencial, como contraseñas, nombres de usuario, números de tarjetas de crédito u otra información confidencial o personal.

Los ataques de phishing usualmente se realizan mediante el envío de correos electrónicos o mensajes fraudulentos que parecen ser de una fuente legítima para engañar a los usuarios. Estos correos electrónicos o mensajes contienen enlaces a sitios web falsos que imitan la apariencia de sitios legítimos, como bancos, redes sociales o plataformas de correo electrónico.

Una vez ingresado en el sitio web falso, se le solicita que ingrese su nombre de usuario y contraseña, una vez que se ingresa esta información, los actores de amenaza la capturan y la utilizan para

acceder ilegalmente a sus cuentas.

2.2.2. Baiting

El baiting es una técnica utilizada para engañar a las personas, esta técnica se basa en la curiosidad y el deseo natural de las personas de obtener algo a cambio, como regalos, descuentos o una descarga gratuita.

El baiting lanza señuelos atractivos que son colocados en comentarios dentro de una publicación, enviado por mensajes o enviados como un anuncio de publicidad de empresas de apariencia legítima, que llevan a las personas a realizar acciones para comprometer su seguridad, como la instalación de software con malware o la solicitud de información personal (fecha de nacimiento, correo electrónico, entre otras) o confidencial (contraseñas o número de tarjetas de débito o crédito).

2.2.3. Filtración de datos

La filtración de datos es un evento en el cual la información confidencial o sensible se divulga, se accede o se comparte de manera no autorizada, ya sea intencional o accidentalmente, lo que resulta útil para atacantes, ya que podrían usar la información para acceder o tratar de acceder a cuentas legítimas para realizar campañas de ataque, como campañas de phishing, desprestigio u otras actividades delictivas, hacia otras personas o entidades.

2.2.4. Malware

El malware es un tipo de software diseñado con la intención de causar daño, robar información o realizar acciones no autorizadas en un sistema informático, dispositivo o red. El malware puede manifestarse en diversas formas, como virus, gusanos, troyanos, spyware y ransomware, entre otros.

Su propósito principal es comprometer la integridad, confidencialidad y disponibilidad de los datos y sistemas, así como también comprometer la privacidad de los usuarios al robar datos sensibles o realizar acciones no autorizadas por el usuario.

2.2.5. Ingeniería social

La ingeniería social es una técnica de manipulación que busca engañar a las personas para obtener información confidencial, acceso a sistemas informáticos o realizar acciones que beneficien al atacante. En lugar de depender de vulnerabilidades técnicas, la ingeniería social explora las debilidades humanas, como la confianza, la curiosidad o el miedo para lograr sus objetivos.

2.2.6. Fuerza bruta

La fuerza bruta es un método utilizado en seguridad informática para intentar encontrar una contraseña o encontrar una clave criptográfica probando exhaustivamente todas las combinaciones

posibles de caracteres, números y símbolos. Es un enfoque simple pero intensivo que implica probar cada posible combinación hasta que se encuentre la correcta.

Si se utilizan contraseñas cortas o débiles (una contraseña débil es una contraseña que carece de complejidad como ser: “password”, “contraseña”, “123456”, entre otras) un ataque de fuerza bruta puede obtener con facilidad la contraseña.

2.2.7. Software no confiable

El software no confiable se refiere a programas informáticos cuya fuente, integridad o seguridad no puede ser garantizada o verificada de manera adecuada. Por lo general, este software ha sido modificado para evadir las medidas de protección y las licencias legales, a menudo contienen malware, que posteriormente será aprovechada para vulnerar la seguridad del dispositivo donde se instaló.

2.2.8. Wi-Fi públicos

Los actores de amenaza podrían implementar redes Wi-Fi públicas y de fácil acceso (una red Wi-Fi que no requiere contraseña para conectarse a la misma) para interceptar datos confidenciales o sensibles, mediante el uso de herramientas de captura de paquetes y programas que permiten ver la comunicación entre los dispositivos y el punto de acceso. Estas redes Wi-Fi son, por lo general, implementadas en lugares de mayor concurrencia como ser aeropuertos, lugares de ocio, centros de comercio u otros lugares públicos para tener un mayor probabilidad de éxito para obtener credenciales u otros datos sensibles.

Los dispositivos móviles suelen ser el objetivo de este tipo de ataques ya que algunos de estos dispositivos tienen la capacidad de conectarse automáticamente a una red que no requiera contraseña y con ello establecer una conexión entre el dispositivo y el punto Wi-Fi sin necesidad de la interacción del usuario.

3. Vulnerabilidades

Una vulnerabilidad es la ausencia o deficiencia presente en las tecnologías de información y comunicación, así también en las personas. Las cuales son aprovechadas por los actores de amenaza para vulnerar la seguridad de los sistemas de información. A continuación se enumeran las principales vulnerabilidades.

3.1. Contraseña corta e insegura

Una contraseña corta e insegura es aquella que carece de complejidad y longitud suficiente para proteger el acceso a una cuenta o sistema contra ataques de diccionario, fuerza bruta o técnicas de descifrado. Las contraseñas cortas suelen ser fáciles de adivinar o descifrar para los actores de amenaza, ya que contienen pocos caracteres y no incluyen una combinación de letras (mayúsculas y

minúsculas), números y caracteres especiales, como ser: “password”, “contraseña”, “123456”,”abc123”, entre otras. Estas contraseñas son altamente vulnerables y representan un riesgo significativo para la seguridad de las cuentas y la información personal.

3.2. Reutilización de contraseñas

La reutilización de contraseñas es un hábito de usar la misma contraseña para múltiples cuentas o servicios en línea. Este comportamiento es peligroso porque si una de las cuentas se ve comprometida, todas las demás cuentas que comparten la mimas contraseña también estarán en riesgo.

Los actores de amenaza pueden aprovecharse de esta práctica para acceder a varias cuentas de un usuario, comprometer su privacidad, robar información confidencial o realizar actividades maliciosas en su nombre. La reutilización de contraseñas aumenta la probabilidad de éxito de un ataque y debilita la seguridad en línea del usuario.

3.3. Resguardo inseguro de la contraseña

Si tenemos la contraseña anotado en un papel dejado en el escritorio, pegado a la pantalla del monitor, guardado en el navegador, guardado en un archivo con nombre “contraseñas” en el computador que no tiene contraseña o se deja el computador sin bloqueo al momento de dejar el escritorio. Existe una alta probabilidad de que alguien conozca la contraseña y se registre un incidente de acceso ilegítimo a la cuenta.

3.4. Software desactualizado

Al utilizar aplicaciones, sistemas operativos o programas informáticos que no han sido actualizados con las últimas versiones disponibles, existe el riesgo de ser victimas de un ataque ya que las actualizaciones contienen correcciones de seguridad, mejoras de rendimiento y nuevas funcionalidades. La falta de actualización puede dejar al software vulnerable a exploits de seguridad, ya que los actores de amenaza pueden aprovecharse de las vulnerabilidades conocidas en versiones antiguas para realizar ataques, comprometer la integridad del sistema o robar información.

3.5. Falta de control de cuentas administrativas

Al asignar múltiples cuentas administrativas, se aumenta la probabilidad de éxito de un ataque y dependerá del cuidado de cada administrador en relación a la protección de la cuenta. Esto implica que si una cuenta se ve comprometida, los actores de amenaza podrían tener acceso no autorizado de la cuenta y quitar u otorgar el acceso a otras cuentas fuera de nuestro ámbito de control.

3.6. Configuraciones predeterminadas

No es recomendable mantener las configuraciones predeterminadas en una cuenta o servicio en línea, debido a que estas configuraciones pueden carecer de seguridad y no podrían ser las adecuadas para proteger la privacidad y la seguridad de la información personal.

Las configuraciones predeterminadas suelen ser genéricas y están diseñadas para satisfacer las necesidades generales de la mayoría de los usuarios, pero no tienen en cuenta las preferencias individuales o las necesidades de seguridad especificas, como ser:

- Autenticación de doble factor.
- Control de inicio de sesión.
- Restricción de la visualización de datos personales (nombre completo, fecha de nacimiento, ubicación de residencia, entre otras).
- Interacción de la cuenta con otras de manera no deseada (visualización de información personal, fotos o videos compartidos y las preferencias del usuario)

3.7. Falta de políticas de seguridad

La falta de políticas de seguridad representa un riesgo significativo debido a la ausencia de protocolos para proteger las contraseñas y cuentas de una entidad. Esto puede incluir:

- Uso de contraseñas cortas, débiles o predecibles
- Falta de autenticación de doble factores
- Uso de la misma contraseña para diferentes plataformas en línea
- Ignorar las actualizaciones de seguridad de los dispositivos

Las políticas de seguridad son fundamentales porque establecen las directrices, procedimientos y normas que regulan el comportamiento de los usuarios y la protección de nuestra información.

3.8. Cultura de ciberseguridad débil

Al igual que en otros aspectos de la vida, se tiene que mostrar interés por la seguridad en línea. En la era digital actual donde todos nos encontramos conectados, depende de cada uno hacer que la conexión en línea sea más segura.

Si no se cuenta con una cultura de ciberseguridad, se presentan los siguientes consejos de seguridad para mantener y mejorar la privacidad de su presencia en línea:

- Configurar las opciones de privacidad y seguridad
- Usar contraseñas robustas utilizando letras en minúscula y mayúscula, números y caracteres especiales.
- No almacenar las contraseñas en el navegador
- Contar con un factor de doble autenticación
- No responder a mensajes de personas o entidades desconocidas

- No conectarse a redes de Wi-Fi abiertas
- Mantener los dispositivos que se conectan en línea actualizados

Con la implementación de estos consejos se tendrá una presencia más segura en línea.

3.9. Uso de dispositivos compartidos

El uso de dispositivos compartidos provoca una falta de privacidad y control individual de la información que se almacene en el mismo. Esto implica que si uno de los usuarios realiza acciones que comprometan la seguridad del dispositivo, los demás usuarios también serán víctimas del ataque.

4. Incidentes

Los incidentes de seguridad son el resultado de la explotación exitosa de determinadas vulnerabilidades por actores de amenaza y estos tienen un impacto en la seguridad de los datos, daño a la imagen institucional entre otros, a continuación se describen los incidentes más comunes dentro del contexto de redes sociales:

4.1. Acceso no autorizado

Un acceso no autorizado ocurre cuando un actor de amenaza logra ingresar a las cuentas sin la debida autorización del usuario legítimo. Este suceso puede implicar la violación de la confidencialidad, integridad o disponibilidad de la información, y puede tener repercusiones significativas en la seguridad y operatividad de una entidad.

4.2. Secuestro y/o pérdida del acceso

Los ataques dirigidos hacia las contraseñas, incluidas las técnicas de ingeniería social, phishing, representan una grave amenaza para la seguridad de nuestras cuentas en línea. Los actores de amenaza pueden obtener acceso no autorizado a nuestras cuentas, comprometiendo nuestra privacidad y seguridad.

Una vez los atacantes tienen acceso a nuestras cuentas, podrían acceder a información personal sensible e incluso modificar nuestras contraseñas y datos de recuperación de la cuenta. Además, podrían exigir un rescate para devolver el control de nuestras cuentas.

Es importante comprender que estos ataques no se limitan únicamente a las redes sociales; también, pueden afectar a otras plataformas en línea. Por lo tanto, es fundamental revisar las configuraciones de seguridad y privacidad disponibles en nuestras cuentas para prevenir este tipo de incidentes.

4.3. Uso indebido de la cuenta

Cuando una cuenta es comprometida por actores de amenaza, estos pueden aprovecharlas para una variedad de actividades maliciosas que comprometen la seguridad y la integridad de la cuenta y de sus seguidores. Las acciones que pueden llevar a cabo incluyen la publicación de contenido inapropiado o dañino, envío de mensajes no deseados o spam, el robo de información personal y campañas de desprestigio o difamación.

4.4. Impacto

El impacto de una cuenta vulnerada trae consecuencias y repercusiones negativas que sufre el usuario legítimo de la misma y posiblemente otros usuarios que interactúan con la misma. Los impactos pueden variar dependiendo de la gravedad de la vulneración de la cuenta, estos incluyen:

4.4.1. Daño a la imagen institucional

El impacto de una cuenta institucional comprometida puede tener un impacto duradero en la reputación de la organización, las críticas negativas pueden dañar la percepción pública de la institución.

4.4.2. Desconfianza de la población

El impacto en la población genera desconfianza en las acciones, declaraciones o integridad de una persona o institución. Cuando la población desconfía de una institución, puede manifestarse en un falta de cooperación, apoyo disminuido, escepticismo hacia las afirmaciones o acciones de la institución y en algunos casos, protestas y descontento.

4.5. Respuesta

Cuando nos enfrentamos a la vulneración de nuestra cuenta, resulta crucial actuar de manera inmediata para recuperar el control y reducir al mínimo las posibles consecuencias negativas que puedan derivarse de la pérdida del control de la cuenta.

4.5.1. Recuperación del acceso

Para recuperar una cuenta en Facebook, se debe realizar la siguientes pasos:

- Ve a la página “Recupera tu cuenta” en https://facebook.com/login/identify/ y sigue las instrucciones. Asegurando de usar una computadora o un teléfono celular con el que se haya iniciado sesión anteriormente en la cuenta de Facebook.

- Buscar la cuenta que se quiere recuperar. Se puede hacer la búsqueda por nombre, dirección de correo electrónico o número de teléfono.
- Seguir los pasos en la pantalla para restablecer la contraseña de la cuenta.

5. Prevención

Una vez conocidos los riegso, es posible implementar acciones preventivas para reducir la probabilidad de un ataque exitoso contra nuestras cuentas en línea. A continuación, se presentan algunas medidas preventivas para garantizar la seguridad en línea.

5.1. Establecer políticas de seguridad

5.1.1. Cuenta institucional

- Toda cuenta debe estar registrada a nombre de la institución
- Las cuentas deben estar vinculadas a un único teléfono y correo electrónico
- El número de teléfono y equipo móvil debe ser propiedad de la institución y asignado a la unidad organizacional responsable de las cuentas. Su uso debe limitarse para tal fin.
- La dirección de correo electrónico vinculado a la cuenta debe ser institucional y asignado a la unidad organizacional responsable de la administración de la cuenta.

5.1.2. Verificación de la cuenta

Para verificar la cuenta se debe realizar las siguientes acciones:

- Completar el perfil: Asegurarse de que el perfil de Facebook tenga toda la información posible.
- Utilizar una foto de perfil y de portada: Estas fotos deben ser claramente identificables.
- Solicitar la verificación de Facebook: Para ello se debe ir a la sección **Configuración** y luego ir a la opción **General**. Luego en la sección **Verificación** seleccionar **Verificar esta página**. Finalmente, seguir las instrucciones para enviar la solicitud de verificación.

5.1.3. Desvinculación del personal

- El servidor público responsable de la(s)cuenta(s) al momento de su desvinculación de la institución, debe entregar las contraseñas de las cuentas, de los dispositivos, del correo electrónico vinculado a la cuenta cuándo corresponda a su inmediato superior o mediante procedimientos internos de la institución a quién corresponda.
- Cuándo se produzca una desvinculación de personal, todas las contraseñas de las cuentas deben ser cambiadas incluyendo la del correo electrónico, cierre de todos los inicios de sesión, revocar y actualizar el acceso a aplicaciones de terceros.

5.2. Habilitar características de seguridad

5.2.1. 2FA

- Iniciar sesión en Facebook

- Dirigirse a la siguiente dirección:

  https://accountscenter.facebook.com/password_and_security/
- En la sección **Contraseña y seguridad,** seleccionar **Autenticación en dos pasos.**
- Para este caso seleccionaremos la opción **APP de autenticación**
- Una vez seleccionado se habilitará un código QR para la habilitación del código MFA en nuestro dispositivo móvil (la aplicación puede ser Authenticator de Google o de Microsoft)
- Una vez escaneado el código con la aplicación se deberá de introducir el código generado en la aplicación
- Una vez finalizado el anterior paso nos pedirá nuevamente nuestra contraseña de Facebook y se activará la Autenticación en dos pasos

5.2.2. Notificación de alertas de seguridad

- Iniciar sesión en Facebook
- Ir a la dirección: https://accountscenter.facebook.com/password_and_security
- Seleccionar **Contraseña y seguridad**
- En la opción **Controles de seguridad** seleccionar **Alertas de inicio de sesión**
- Seleccionar la cuenta a se notificada
- Seleccionar el correo vinculado a la cuenta y cerrar

5.2.3. Establecer roles y permisos

- Inicia sesión en Facebook y, luego, haz clic en la foto del perfil en la parte superior derecha.
- Haz clic en **Ver todos los perfiles** y luego selecciona la página a la que quieres cambiar.
- Haz clic en la foto del perfil de la página en la parte superior derecha para ir a tu página.
- Haz clic en **Administrar** y, luego, en **Acceso a la página** a la izquierda, debajo de **Tus herramientas**.
- Junto a **Personas** con acceso a Facebook, haz clic en **Agregar**.
- Haz clic en **Siguiente**, escribe el nombre o la dirección de correo electrónico de la persona a la que quieres otorgar acceso a Facebook y haz clic en su nombre.

- Desde aquí, puedes elegir otorgar acceso a Facebook con control total o parcial:
  - Para otorgar acceso a Facebook con control parcial: desplázate hacia abajo y haz clic en **Otorgar acceso**.
  - Para otorgar a Facebook con control total: desplázate hacia abajo, haz clic en

    para que la persona tenga control total y, luego, haz clic en **Otorgar acceso.**
- Escribe tu contraseña de Facebook y haz clic en **Confirmar.**

Existen 6 roles en Facebook las cuales pueden ser delegadas:

Roles de la versión clásica para páginas	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

Eliminar el acceso a Facebook o tareas de una persona

Inicia sesión en Facebook y, luego, haz clic en la foto del perfil en la parte superior derecha.

- Haz clic en **Ver todos los perfiles** y luego selecciona la página a la que quieres cambiar.
- Haz clic la foto del perfil de la página en la parte superior derecha para ir a tu página.
- Haz clic en **Administrar** y, luego, en **Acceso a la página** a la izquierda, debajo de **Tus herramientas**.
- Junto a la persona que quieras eliminar, haz clic en ••• y, luego, en **Eliminar de la página**.

5.3. Gestión segura de contraseñas

5.3.1. Contraseña robusta y única

Las contraseñas robustas son más difíciles de adivinar o descifrar mediante ataques de fuerza bruta, ingeniería social u otros métodos utilizados por los actores de amenaza. Al elegir contraseñas complejas y únicas, se aumenta significativamente la seguridad de la cuenta y reduce el riesgo de acceso no autorizado.

5.3.2. Cambiar la contraseña periódicamente

Cambiar la contraseña periódicamente es un práctica de seguridad recomendada, esto reduce el riesgo de acceso no autorizado a nuestras cuentas. Esta medida ayuda especialmente cuando las plataformas en línea son víctimas de un ataque y sufren una filtración de datos, lo que compromete la seguridad de nuestras contraseñas con las que iniciamos sesión dentro de la misma.

Al cambiar periódicamente nuestra contraseña, reducimos el riesgo de éxito para que los actores de amenaza utilicen las contraseñas filtradas para acceder a nuestras cuentas.

5.3.3. Gestor de contraseñas

Los gestores de contraseñas son herramientas útiles y beneficiosas, permiten la gestión de contraseñas al almacenarlas en un único lugar seguro fuera del navegador, escritas en un papel o almacenadas dentro de un archivo de texto, otro beneficio que se obtiene con el gestor de contraseñas es la generación de contraseñas complejas y seguras para cada cuenta que se vaya almacenando.

5.4. Deshabilitar aplicaciones de terceros conectados a la cuenta

Algunas aplicaciones de terceros pueden solicitar permisos amplios para acceder a la información de la cuenta. Esto puede incluir datos sensibles como correos electrónicos, contactos, historial de ubicaciones, entre otros. Al deshabilitar estas aplicaciones, se protege la privacidad del usuario y se limita el acceso no deseado a la información personal.

Estas aplicaciones también pueden tener vulnerabilidades de seguridad que podrían ser explotadas por actores de amenazas para acceder a la cuenta y comprometer la información personal del usuario.

5.5. Revisar periódicamente roles y permisos

Es importante revisar periódicamente los roles y permisos de una página, para garantizar la seguridad y la integridad de la cuenta, así como para mantener un control adecuado sobre quién tiene acceso y que tipo de acciones puede realizar.

Con esta acción se reduce el riesgo de accesos no autorizados, controlar la gestión de la página y proteger la reputación de la entidad al revisar las publicaciones que se van realizando.

5.6. Cuidado con enlaces y software sospechoso

Es recomendable no abrir enlaces de origen desconocido o sospechoso debido a las amenazas que pueden representar para la seguridad y privacidad en línea. Esto permite protegerse contra el malware, el phishing y otros ataques que pueden ser diseminados a través de enlaces de origen desconocido o sospechoso.

Asimismo, es recomendable no instalar aplicaciones o software sospechoso debido a que la mayoría de estos contienen malware, que posteriormente será aprovechada para vulnerar la seguridad el dispositivo donde se instaló.

5.7. Cierre de sesión en computadoras compartidas

Una práctica segura es el cierre de sesión en computadoras compartidas para proteger la privacidad y la seguridad de la información personal. Al cerrar la sesión, se evita que otras personas accedan a cuentas personales, correos electrónicos, redes sociales u otros servicios en línea que hayan sido

utilizados durante la sesión. Es recomendable eliminar todo el historial realizado durante la navegación en línea, registro de cookies o de otra información que llega a almacenarse en estos dispositivos compartidos.

6. Herramientas