Comisión Estatal para la Atención y Protección de los Periodistas

SEGURIDAD DIGITAL PARA PERIODISTAS Y PERSONAS DEFENSORAS DE DDHH

Ing. Nohel González López

Xalapa, Veracruz. 3 Mayo de 2024.

Cada vez más y más aspectos de nuestras vidas transcurren en el mundo digital, por la comodidad y ventajas, las cuales no viene sin sus problemas e incluso riesgos.

La seguridad digital es fundamental para los periodistas y actividas, ya que trabajan con información sensible y a menudo enfrentan riesgos de ciberseguridad.

El periodismo está imprimiendo lo que otros no quieren que se imprima, y el riesgo de verse interrumpido electrónicamente nunca ha sido tan grande. Con la accesibilidad cada vez mayor de las herramientas de vigilancia sofisticadas, casi cualquier persona, desde los servicios de seguridad a nivel estatal hasta las corporaciones y los ciberdelincuentes, podría intentar vigilar o interrumpir su trabajo.

Comisión Estatal para la Atención y Protección de los Periodistas

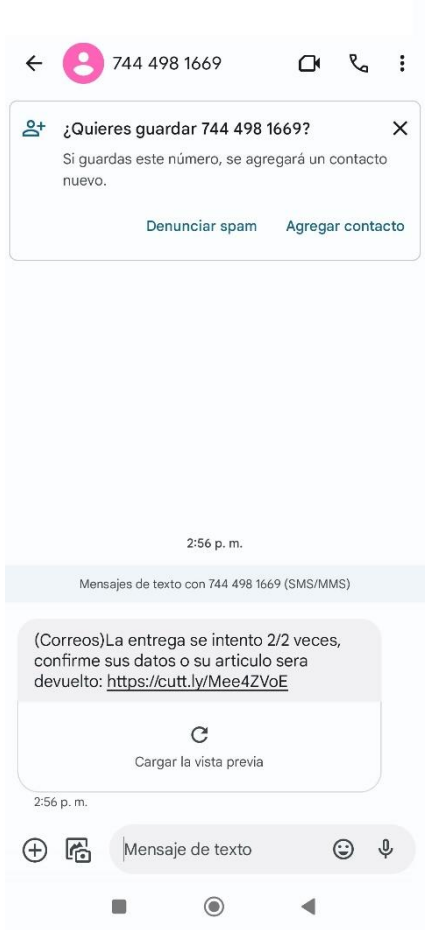
- Evaluación ¿Cómo cuido mi información?, ¿Qué tan segura está?
- Tipos de ataque: Phishing, Malware, Robo de Identidad, Ransomware, vishing o smishing, ingeniería social.
- *Primero lo primero:* generando contraseñas seguras, y su cambio periodico
- Correo de recuperación dedicado
- Registrar la línea telefónica
- ¿Qué es la autenticación de dos factores?
- Asegurando un dispositivo Android e iPhone PIN, Patrón de desbloqueo
- Autentificación de dos factores WhatsApp EJEMPLO
- Autentificación de dos factores Facebook EJEMPLO
- Autentificación de dos factores Gmail EJEMPLO
- Autentificación de dos factores por código, Google Authenticator y Microsoft authenticator
- Cuentas verificadas
- Cifrado de discos Mac y Windows
- RESPALDO, ¿qué es mejor que un respaldo? dos respaldos, y respaldo en frio/offline
- Dispositivos de segunda mano, y reparaciones, riesgos y precauciones
- Exportar tus cuentas al restaurar de fabrica
- Conectándome en lugares públicos
- Asegurando mi red inalámbrica, robo de WiFi es lo de menos ARP Spoofing
- La IA una nueva amenaza, clonado de voz y palabras clave
- “Apps de facebook

Comisión Estatal para la Atención y Protección de los Periodistas

El phishing es una forma de fraude en línea en la que los estafadores intentan engañar a las personas para que revelen información personal, como contraseñas, números de tarjetas de crédito o información bancaria, haciéndose pasar por entidades de confianza, como bancos, empresas o servicios en línea. Usualmente, los estafadores envían correos electrónicos, mensajes de texto o mensajes instantáneos que parecen legítimos y persuaden a la víctima para que haga clic en un enlace malicioso que los lleva a un sitio web falso, donde se les pide que ingresen su información personal. Esta información se utiliza luego para cometer fraude, robar identidades o realizar transacciones no autorizadas.

NOTA: ante una duda, cualquier problema resuélvanlo dentro de la aplicación

Comisión Estatal para la Atención y Protección de los Periodistas



Comisión Estatal para la Atención y Protección de los Periodistas

El malware es un término que se refiere a software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario. Hay varios tipos de malware, incluyendo virus, gusanos, troyanos, ransomware, spyware y adware, entre otros. Cada tipo tiene sus propios métodos y objetivos, pero todos comparten la intención de causar daño, robar información o controlar sistemas sin autorización.

El ransomware cifra los archivos del usuario y exige un rescate para restaurar el acceso.

Comisión Estatal para la Atención y Protección de los Periodistas

El "vishing" es una forma de estafa telefónica que implica la manipulación psicológica de las personas para obtener información confidencial, como números de tarjetas de crédito, contraseñas u otra información personal. El término "vishing" proviene de la combinación de las palabras "voice" (voz) y "phishing" (un tipo de estafa en línea que implica engañar a las personas para que revelen información confidencial).

El "smishing" es una forma de estafa que se lleva a cabo a través de mensajes de texto SMS (Short Message Service) o mensajes de texto en aplicaciones de mensajería instantánea. El término "smishing" proviene de la combinación de las palabras "SMS" y "phishing".

Comisión Estatal para la Atención y Protección de los Periodistas

El hackeo y el robo de identidad son dos tipos de actividades delictivas en el ámbito digital, pero difieren en sus enfoques y objetivos.

1.Hackeo:

1. El hackeo se refiere al acceso no autorizado a sistemas informáticos, redes o dispositivos.

2.Robo de identidad:

1. El robo de identidad implica el uso fraudulento de la información personal de una persona sin su consentimiento.

Comisión Estatal para la Atención y Protección de los Periodistas

Crear una contraseña segura es crucial para proteger tus cuentas en línea contra el acceso no autorizado. Aquí tienes algunos consejos para crear contraseñas seguras:

Longitud:

Las contraseñas más largas suelen ser más seguras. Se recomienda que tengan al menos 12 caracteres de longitud, pero idealmente más.

Complejidad:

Usa una combinación de letras (mayúsculas y minúsculas), números, y caracteres especiales (como !, @, #, $, %, etc.).
Evita secuencias obvias o palabras comunes que puedan ser adivinadas fácilmente.

Evita información personal:

No utilices información personal fácilmente accesible o predecible, como tu nombre, fecha de nacimiento, nombres de familiares o mascotas, números de teléfono, etc.

No reutilices contraseñas:

Utiliza contraseñas únicas para cada cuenta en línea que tengas. Esto evita que un acceso comprometido a una cuenta exponga otras cuentas.

Evita patrones simples:

Evita secuencias simples o patrones obvios en tus contraseñas, como "123456", "abcdef", "qwerty", etc.

Considera el uso de frases de contraseña:

Una opción es crear una frase de contraseña compuesta por palabras aleatorias que tengan un significado solo para ti, y luego modificarla con números y caracteres especiales. Por ejemplo: "C@saBl4nc@EsM1C0ntr@s3ñ@"

Utiliza un gestor de contraseñas:

Considera utilizar un gestor de contraseñas confiable para generar y almacenar contraseñas seguras de forma segura. Esto te permite tener contraseñas únicas y complejas para cada cuenta sin tener que recordarlas todas.

Comisión Estatal para la Atención y Protección de los Periodistas

Correo de recuperación dedicado:

Correo electrónico cuyo principal fin de recuperar el acceso a mi cuentas o a mi correo de uso principal u otras cuentas, y que no uso para el día a día.

Comisión Estatal para la Atención y Protección de los Periodistas

2FA

La 2FA, o autenticación de dos factores, es un método de seguridad que requiere dos formas distintas de verificar la identidad de un usuario antes de permitir el acceso a una cuenta o sistema en línea. Este método añade una capa adicional de seguridad más allá de la contraseña tradicional. Los dos factores típicamente utilizados en la autenticación de dos factores son:

Algo que sabes: Este es el factor de conocimiento, generalmente la contraseña. Es algo que el usuario conoce y utiliza para demostrar su identidad.

Algo que tienes: Este es el factor de posesión, que implica algo físico que el usuario posee, como un teléfono móvil, una tarjeta de seguridad, un token físico o una aplicación de autenticación en el dispositivo móvil.

La 2FA funciona de la siguiente manera:

Cuando un usuario intenta iniciar sesión en una cuenta protegida con 2FA, primero deberá ingresar su nombre de usuario y contraseña como de costumbre.

Después de ingresar la contraseña, se le solicitará al usuario que proporcione un segundo factor de autenticación, que puede ser un código generado por una aplicación de autenticación en su teléfono móvil, un código enviado por mensaje de texto (SMS), una clave de seguridad física (como una llave USB de seguridad), o incluso una huella digital o reconocimiento facial en algunos casos.

Una vez que el usuario proporciona con éxito el segundo factor de autenticación, se le permite el acceso a la cuenta.

La 2FA ayuda a proteger las cuentas en línea incluso si la contraseña es comprometida, ya que un atacante necesitaría acceso al segundo factor (que generalmente está en posesión física del usuario) para poder acceder a la cuenta. Esto mejora significativamente la seguridad de las cuentas en línea y ayuda a prevenir el acceso no autorizado.

Comisión Estatal para la Atención y Protección de los Periodistas

Asegurando mi Whatsapp:

Comisión Estatal para la Atención y Protección de los Periodistas

Asegurando mi Facebook:

Para activar o administrar la autenticación en dos pasos

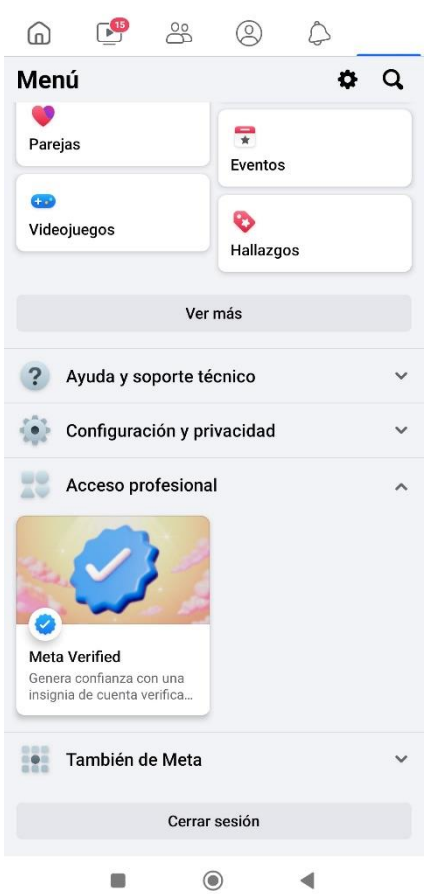
1.Haz clic en tu foto del perfil en la parte superior derecha y, luego, en **Configuración y privacidad**.
2.Haz clic en **Configuración**.
3.Haz clic en **Centro de cuentas** y, luego, en **Contraseña y seguridad**.
4.Haz clic en **Autenticación en dos pasos** y selecciona la cuenta que quieres actualizar.
5.Elige el método de seguridad que quieras agregar y sigue las instrucciones que aparecen en pantalla.

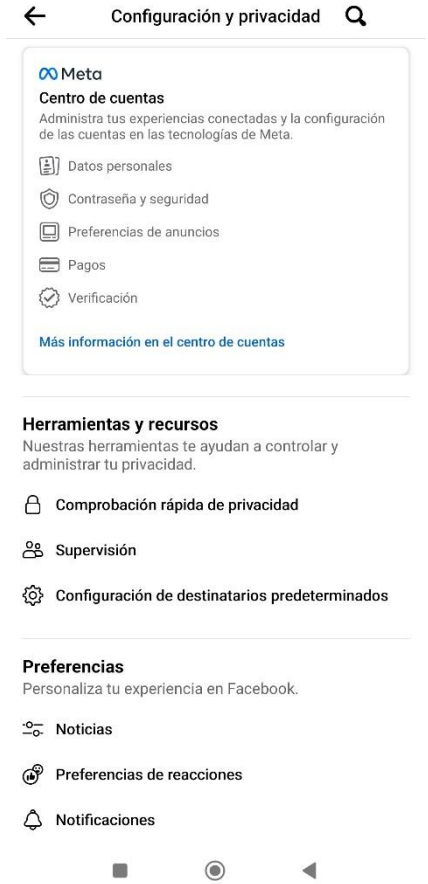
Cuando configures la autenticación en dos pasos en Facebook, se te solicitará que elijas uno de los tres métodos de seguridad:

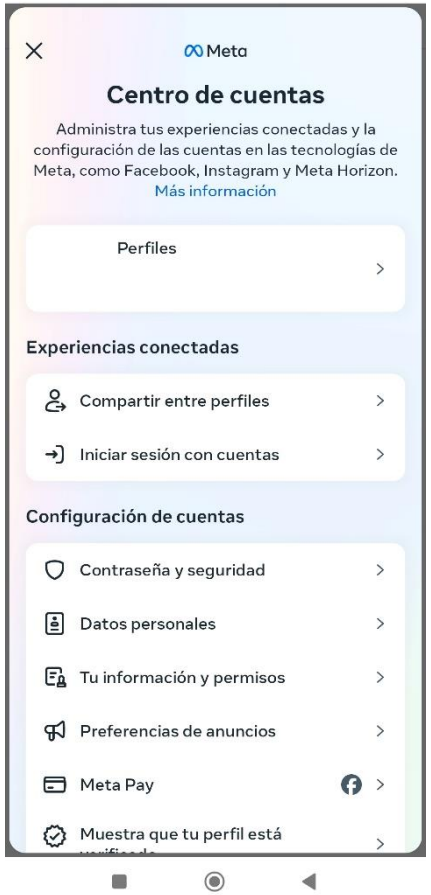
•Ingresar tu clave de seguridad en un dispositivo compatible.
•Códigos de inicio de sesión de una app de autenticación de terceros.
•Códigos de mensaje de texto (SMS) del teléfono celular.

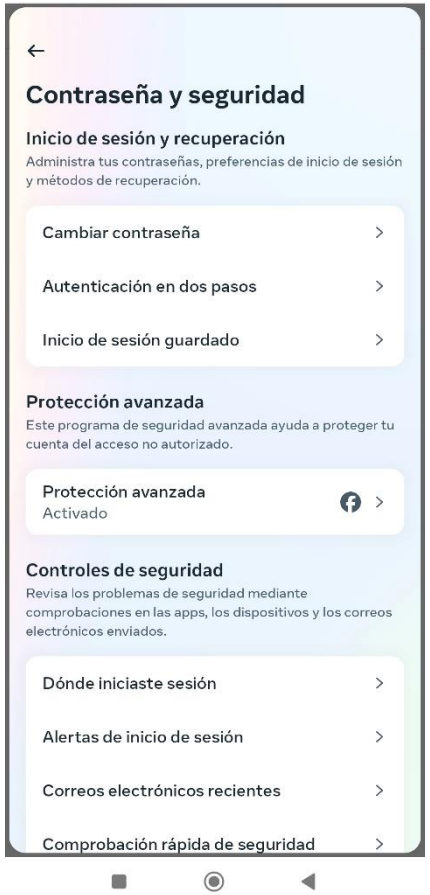
Una vez que actives la autenticación en dos pasos, podrás recibir diez códigos de inicio de sesión para usar cuando no puedas utilizar el teléfono.

Comisión Estatal para la Atención y Protección de los Periodistas



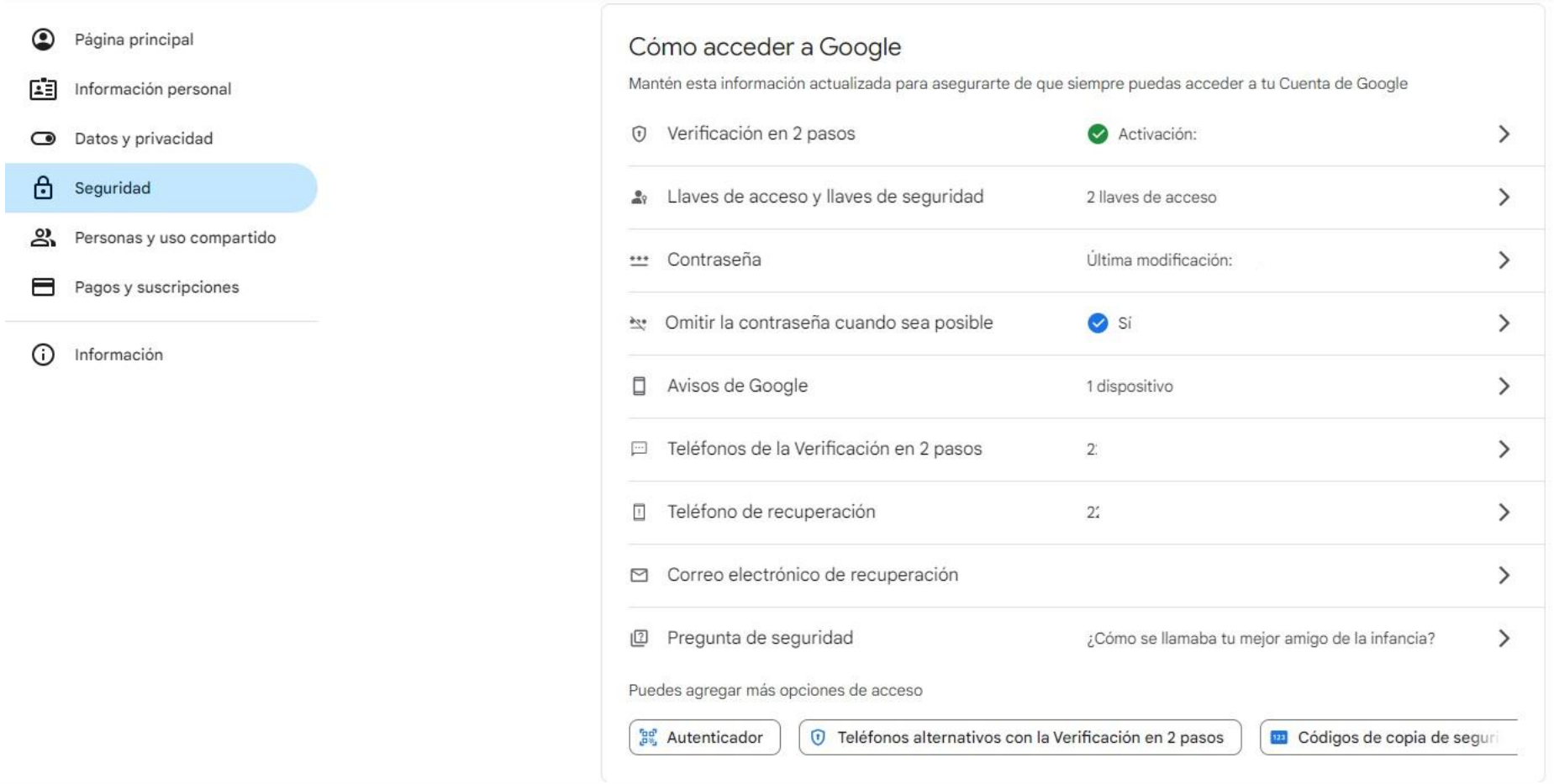






Comisión Estatal para la Atención y Protección de los Periodistas

Asegurando mi Gmail:



Comisión Estatal para la Atención y Protección de los Periodistas

Google Authenticator es una aplicación de teléfono móvil que proporciona un segundo nivel de verificación de la identidad, también conocido como autenticación de dos factores (2FA). Su función principal es agregar una capa adicional de seguridad a las cuentas en línea al requerir no solo una contraseña para iniciar sesión, sino también un código de verificación generado por la aplicación.

El funcionamiento básico de Google Authenticator es el siguiente:

Configuración inicial:

Primero, el usuario debe configurar la autenticación de dos factores en su cuenta en línea, como por ejemplo, en una cuenta de Google, Facebook, Twitter, etc.
Durante la configuración, el usuario vincula su cuenta en línea con la aplicación Google Authenticator escaneando un código QR proporcionado por el servicio en línea o ingresando una clave secreta.

Generación de códigos:

Después de la configuración inicial, cada vez que el usuario intenta iniciar sesión en su cuenta en línea, además de la contraseña habitual, se le pedirá que ingrese un código de verificación.
Este código de verificación es generado por Google Authenticator y cambia cada pocos segundos.
El usuario simplemente abre la aplicación Google Authenticator en su dispositivo móvil y ve el código de verificación actual.

Verificación:

El usuario ingresa este código de verificación en el sitio web o la aplicación donde está intentando iniciar sesión.
Este código es temporal y es válido solo por un corto período de tiempo (generalmente unos pocos segundos).
Una vez que el código es verificado correctamente, se concede el acceso a la cuenta en línea.

La principal ventaja de Google Authenticator es que incluso si un atacante logra obtener la contraseña del usuario, aún así necesitaría el código de verificación generado por la aplicación en el dispositivo móvil del usuario para acceder a la cuenta. Esto proporciona una capa adicional de seguridad significativa y ayuda a proteger las cuentas en línea contra el acceso no autorizado.

Comisión Estatal para la Atención y Protección de los Periodistas

Para los dispositivos iPhone, existe una alternativa a Google Authenticator llamada "Authenticator" de Microsoft. Funciona de manera similar a Google Authenticator, proporcionando códigos de verificación de dos factores para cuentas en línea.
Aquí hay un resumen de cómo funciona:

Configuración inicial:

Al igual que con Google Authenticator, durante la configuración inicial de la autenticación de dos factores en una cuenta en línea, puedes escanear un código QR o ingresar una clave secreta en la aplicación Authenticator en tu iPhone.

Generación de códigos:

Una vez que hayas vinculado tu cuenta en línea con la aplicación Authenticator, la aplicación generará códigos de verificación de dos factores.

Verificación:

Cuando intentes iniciar sesión en tu cuenta en línea, además de tu contraseña, se te pedirá que ingreses el código de verificación generado por la aplicación Authenticator en tu iPhone.

Abres la aplicación Authenticator en tu iPhone y copias el código de verificación actual que se muestra.

Luego, ingresas este código de verificación en el sitio web o la aplicación donde estás intentando iniciar sesión.

La aplicación Authenticator de Microsoft está disponible de forma gratuita en la App Store de Apple y es una opción popular para agregar una capa adicional de seguridad a tus cuentas en línea si estás utilizando un iPhone.

Comisión Estatal para la Atención y Protección de los Periodistas

Para cifrar un disco en Windows, puedes utilizar una herramienta integrada llamada BitLocker. BitLocker es una función de cifrado de disco completo disponible en ciertas ediciones de Windows (como Windows 10 Pro, Enterprise y Education). Te guiaré a través de los pasos básicos para cifrar un disco utilizando BitLocker:

Abre el Explorador de archivos:

Haz clic derecho en la unidad que deseas cifrar (por ejemplo, la unidad C:) y selecciona "Activar BitLocker".

Configura BitLocker:

Se te presentará una ventana que te preguntará cómo deseas desbloquear el disco. Puedes elegir entre "Usar una contraseña" o "Usar un dispositivo de almacenamiento USB". Selecciona una opción y sigue las instrucciones para configurarla.

Copia o imprime la clave de recuperación:

BitLocker te proporcionará una clave de recuperación que puedes utilizar en caso de que olvides tu contraseña. Es importante guardar esta clave en un lugar seguro, como una unidad USB o una impresión física.

Inicia el proceso de cifrado:

Una vez que hayas configurado la opción de desbloqueo y guardado la clave de recuperación, puedes iniciar el proceso de cifrado. BitLocker comenzará a cifrar el disco y este proceso puede llevar algún tiempo, dependiendo del tamaño y la velocidad del disco.

Finaliza el proceso:

Una vez que el cifrado esté completo, la unidad estará protegida y BitLocker estará activado. De ahora en adelante, cada vez que inicies tu computadora, se te pedirá que ingreses la contraseña o insertes el dispositivo USB para desbloquear el disco.

Es importante tener en cuenta que BitLocker no está disponible en todas las ediciones de Windows, por lo que es posible que necesites verificar si tu versión de Windows es compatible. Además, BitLocker solo cifra unidades de datos; para cifrar el disco del sistema operativo, deberás usar una versión específica de Windows que admita esta función o buscar alternativas de cifrado de disco de terceros.

Comisión Estatal para la Atención y Protección de los Periodistas

En macOS, puedes cifrar los discos utilizando una función integrada llamada FileVault. FileVault es una herramienta de cifrado de disco completo que protege los datos almacenados en tu Mac al cifrar todo el disco usando tecnología de cifrado de nivel militar.

Aquí te muestro cómo activar FileVault y cifrar un disco en macOS:

Abre Preferencias del Sistema:

Haz clic en el icono de Apple en la esquina superior izquierda de la pantalla y selecciona "Preferencias del Sistema".

Accede a Seguridad y Privacidad:

En Preferencias del Sistema, haz clic en "Seguridad y Privacidad".

Selecciona la pestaña "FileVault":

Dentro de Seguridad y Privacidad, selecciona la pestaña "FileVault".

Desbloquea la configuración:

Haz clic en el candado en la esquina inferior izquierda de la ventana y proporciona la contraseña de administrador para desbloquear la configuración.

Activa FileVault:

Haz clic en el botón "Desbloquear" si aún no lo has hecho, luego haz clic en "Activar FileVault".

Se te pedirá que elijas cómo deseas desbloquear el disco en caso de que olvides tu contraseña de inicio de sesión. Puedes elegir entre "Usar la contraseña de tu cuenta de iCloud" o "Crear un código de rescate".

Se te pedirá que reinicies tu Mac para iniciar el proceso de cifrado.

Espera a que se complete el cifrado:

El proceso de cifrado puede llevar algún tiempo, dependiendo del tamaño del disco y la velocidad de tu Mac.

Mientras el cifrado está en curso, puedes seguir utilizando tu Mac normalmente, pero ten en cuenta que el rendimiento puede ser un poco más lento durante este tiempo.

Una vez completado el proceso de cifrado, todos los datos en el disco estarán protegidos y solo podrán ser accedidos mediante el inicio de sesión con tu contraseña de usuario o mediante el código de rescate que hayas creado. FileVault es una excelente manera de proteger la información sensible en tu Mac en caso de pérdida o robo del dispositivo.

Comisión Estatal para la Atención y Protección de los Periodistas

La seguridad digital es fundamental para los periodistas, ya que trabajan con información sensible y a menudo enfrentan riesgos de ciberseguridad. Aquí hay algunas medidas de seguridad digital importantes que los periodistas deben considerar:

Usar contraseñas seguras:

Utiliza contraseñas únicas y seguras para todas tus cuentas en línea.

Considera el uso de un gestor de contraseñas para generar y almacenar contraseñas de forma segura.

Autenticación de dos factores (2FA):

Habilita la autenticación de dos factores siempre que sea posible en tus cuentas en línea para agregar una capa adicional de seguridad.

Cifrado de comunicaciones:

Utiliza herramientas de comunicación cifradas, como Signal o WhatsApp, para comunicaciones sensibles.

Usa conexiones seguras (HTTPS) al navegar por sitios web y evita conectarte a redes Wi-Fi públicas no seguras.

Cifrado de dispositivos y archivos:

Cifra tus dispositivos y archivos sensibles utilizando herramientas como FileVault en macOS o BitLocker en Windows.

Considera el uso de herramientas de cifrado de archivos para proteger archivos sensibles almacenados en la nube.

Actualización de software:

Mantén siempre actualizado el software de tus dispositivos y aplicaciones para protegerte contra vulnerabilidades conocidas.

Sensibilización sobre la ingeniería social:

Capacítate y sé consciente de las técnicas de ingeniería social utilizadas por los ciberdelincuentes para engañar a las personas y obtener acceso no autorizado a sistemas o información.

Respaldo de datos:

Realiza copias de seguridad regulares de tus datos importantes en dispositivos externos o servicios en la nube seguros.

Formación en seguridad digital:

Participa en programas de formación en seguridad digital específicamente diseñados para periodistas para aprender mejores prácticas y técnicas de protección.

Protección de fuentes:

Utiliza herramientas de anonimización y protección de fuentes cuando sea necesario para garantizar la seguridad y la confidencialidad de tus fuentes.

Evaluación de riesgos:

Realiza evaluaciones de riesgos periódicas para identificar posibles amenazas y vulnerabilidades en tu entorno digital y toma medidas para mitigarlos.