PROTEGIENDO LA VERDAD: GUÍA DE SEGURIDAD DIGITAL PARA PERIODISTAS Y ACTIVISTAS

PROTEGE TU VOZ Y TU MISIÓN EN UN MUNDO DIGITAL EN CONSTANTE CAMBIO.

TEMPLAR CIBER-SEGURIDAD DE LA INFORMACIÓN S.A.S.

TABLA DE CONTENIDO

03 INTRODUCCIÓN

04 CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

11 CALAS PÍTULO 2: PROTECCIÓN DE LA COMUNICACIÓN Y LAS FUENTES

16 CAPÍTULO 3: SEGURIDAD EN DISPOSITIVOS Y ALMACENAMIENTO

22 CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

28 CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

33 CONCLUSIÓN

34 AGRADECIMIENTOS

INTRODUCCIÓN

En la era digital, el papel de periodistas y activistas es más crucial que nunca. Son ellos quienes sacan a la luz verdades ocultas, denuncian injusticias y defienden los derechos humanos. Sin embargo, esta labor los expone a una serie de amenazas digitales que pueden poner en riesgo su seguridad personal, la confidencialidad de sus fuentes y la integridad de su trabajo.

Este e-book tiene como objetivo proporcionar herramientas, consejos prácticos y estrategias efectivas para que periodistas y activistas puedan protegerse en el entorno digital. A través de esta guía, buscamos empoderarlos para que continúen su labor esencial sin comprometer su seguridad ni la de aquellos que confían en ellos.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

Como periodista o activista, tu labor implica buscar y compartir la verdad, defender derechos y exponer injusticias. Sin embargo, esta misión te coloca en el centro de riesgos digitales que pueden comprometer tu seguridad y la de tus fuentes. Desde ataques de phishing que buscan robar información confidencial, hasta sofisticadas tácticas de vigilancia y ciberacoso que buscan silenciarte, comprender estas amenazas es el primer paso para protegerte. En este capítulo, exploraremos los peligros más comunes que enfrentan periodistas y activistas y te brindaremos herramientas para defender tu labor en un mundo digital cada vez más complejo.

1.1 Ataques de Phishing y Malware

Los Ataques de Phishing

El phishing es una de las tácticas más utilizadas por ciberdelincuentes para engañar a sus objetivos. Este ataque consiste en enviar correos electrónicos, mensajes de texto o llamadas que aparentan provenir de fuentes legítimas, como servicios de correo, redes sociales o incluso contactos conocidos. El objetivo del atacante es lograr que la víctima revele información confidencial (como contraseñas) o instale malware en su dispositivo.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

Técnicas comunes de phishing:

- Correos electrónicos falsificados: Los atacantes envían correos con apariencia legítima, solicitando que la víctima haga clic en un enlace o descargue un archivo. Estos mensajes pueden parecer urgentes o importantes, como alertas de seguridad, solicitudes de actualización de cuentas o incluso mensajes de colegas de confianza.
- Enlaces maliciosos: Estos correos incluyen enlaces que redirigen a sitios web falsos, diseñados para parecerse a servicios reales (como proveedores de correo electrónico, bancos o plataformas de redes sociales). Si la víctima ingresa su información de acceso en estos sitios falsos, el atacante la roba.
- Archivos adjuntos peligrosos: Los archivos adjuntos, como documentos de Word o PDF, pueden contener macros o programas maliciosos que se activan al abrirlos. Una vez ejecutado, el malware puede instalarse en el dispositivo de la víctima, permitiendo el acceso no autorizado.

Los Ataques de Malware

El malware es software malicioso diseñado para dañar o acceder a un sistema sin el consentimiento del usuario. Los ataques de malware pueden ocurrir de varias maneras, como a través de la instalación de spyware para monitorear actividades, ransomware para cifrar y secuestrar archivos a cambio de un rescate, o incluso troyanos que permiten el acceso remoto al dispositivo.

- **Spyware:** Este tipo de malware se instala de forma oculta y permite al atacante acceder a la información del dispositivo, como mensajes de texto, llamadas, correos electrónicos y ubicaciones GPS.
- **Ransomware:** Esta amenaza cifra los archivos del dispositivo y exige un pago para recuperar el acceso. Para un periodista o activista, perder el acceso a documentos y contactos puede significar un golpe devastador a su trabajo.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

- **Troyanos de acceso remoto (RAT):** Estos programas permiten a los atacantes controlar el dispositivo de forma remota. Pueden encender cámaras, micrófonos, descargar archivos y espiar todo lo que ocurre en el sistema.

Medidas de Protección Contra Phishing y Malware

- **Desconfía de mensajes sospechosos:** Si recibes un correo electrónico, mensaje de texto o llamada que solicita información sensible o contiene un enlace/archivo inesperado, verifica la autenticidad del remitente. No hagas clic ni descargues archivos sin confirmar.
- **Usa autenticación de dos factores (2FA):** Configura la autenticación de dos factores para todas tus cuentas importantes. Esto añade una capa de seguridad, ya que necesitarás un segundo código para acceder, incluso si alguien obtiene tu contraseña.
- **Instala software de seguridad:** Utiliza antivirus y antimalware de calidad que puedan detectar y bloquear amenazas en tiempo real. Mantén el software siempre actualizado para protegerte de las últimas vulnerabilidades.

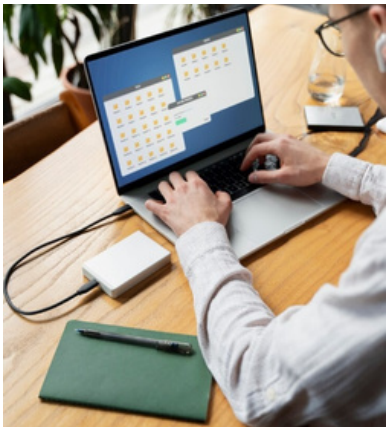
1.2 Vigilancia y Monitoreo Digital

La Amenaza de la Vigilancia Digital

La vigilancia digital es una de las mayores amenazas para periodistas y activistas, especialmente aquellos que trabajan en entornos represivos o

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

investigan temas sensibles. Gobiernos, grupos delictivos y actores con intereses particulares pueden utilizar herramientas avanzadas para monitorear las actividades en línea, interceptar comunicaciones y acceder a información confidencial.



- **Intercepción de comunicaciones:** Las llamadas telefónicas, mensajes de texto y correos electrónicos pueden ser interceptados por actores maliciosos. En algunos casos, las agencias gubernamentales utilizan tecnología de interceptación para espiar a periodistas y activistas que consideran una amenaza.
- **Software espía avanzado:** Herramientas como Pegasus, desarrolladas por empresas especializadas en ciberseguridad ofensiva, pueden instalarse en los dispositivos de una persona y tener acceso total a sus datos, incluyendo mensajes cifrados, correos electrónicos, archivos, llamadas, contactos y ubicaciones.

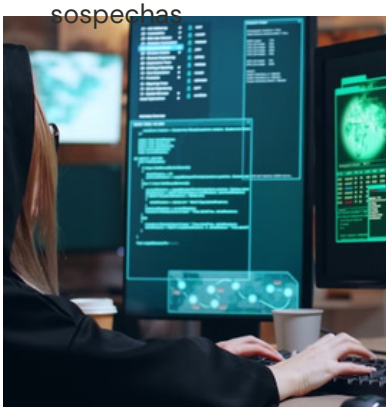
Casos Reales de Vigilancia

- **Periodistas en riesgo:** En 2018, se descubrió que varios periodistas de diferentes países habían sido objetivo del software espía Pegasus, que se instaló en sus teléfonos para monitorear sus actividades, llamadas y mensajes. Este tipo de vigilancia puede comprometer la integridad de sus fuentes y la confidencialidad de sus investigaciones.
- **Activistas en la mira:** Activistas que luchan por los derechos humanos o denuncian corrupción han sido blanco de espionaje por parte de diversos actores que buscan silenciarlos.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

Medidas de Protección Contra la Vigilancia Digital

- Comunicación cifrada: Utiliza aplicaciones de mensajería con cifrado de extremo a extremo (como Signal o Wire) para garantizar que solo tú y tu destinatario puedan leer los mensajes.
- Revisiones periódicas de seguridad: Realiza análisis regulares de tus dispositivos con herramientas de detección de spyware. Si sospechas



que tu dispositivo ha sido comprometido, apaga la conectividad (Wi-Fi, datos móviles y Bluetooth) y busca ayuda de expertos en ciberseguridad.
- Uso de dispositivos seguros: Si trabajas con información extremadamente sensible, considera el uso de un dispositivo dedicado exclusivamente a tus comunicaciones seguras y evita mezclarlo con otras actividades personales.

1.3 Ciberacoso y Campañas de Desinformación

El Ciberacoso Como Herramienta de Intimidación

El ciberacoso busca intimidar, silenciar o desacreditar a periodistas y activistas. Este puede manifestarse a través de amenazas directas, insultos, difamación o campañas de acoso coordinado en redes sociales. Las víctimas de ciberacoso a menudo se enfrentan a un ambiente hostil que puede afectar su salud mental, reputación y, en algunos casos, incluso su seguridad física.

- **Amenazas y acoso directo:** Los ciberacosadores pueden enviar mensajes intimidatorios, hacer comentarios abusivos en redes sociales o difundir rumores con el fin de generar miedo y presionar a la víctima.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

- **Doxing y exposición de información personal:** El doxing consiste en la publicación de información privada o sensible (como direcciones, números de teléfono, familiares) para exponer a la persona al acoso físico y digital.
- **Ataques organizados:** Grupos organizados pueden coordinar campañas de acoso para atacar a periodistas y activistas, generando comentarios negativos masivos, spam, y falsos reportes para silenciar sus cuentas.

Campañas de Desinformación y Noticias Falsas

La desinformación se utiliza para manipular la percepción pública y desacreditar el trabajo de periodistas y activistas. Esto puede incluir la creación de noticias falsas, edición de imágenes y videos (deepfakes), y la difusión de información engañosa para confundir a la audiencia y dañar la reputación de la persona.

- **Creación de perfiles falsos:** Los atacantes pueden crear perfiles que simulan ser de la víctima, difundiendo información errónea y desacreditándola.
- **Difusión de contenido falso:** La manipulación de contenido, como fotos o videos, para distorsionar la realidad o presentar a la persona en una luz negativa.

Medidas de Protección Contra el Ciberacoso y la Desinformación

- **Revisión de privacidad en redes sociales:** Ajusta la configuración de privacidad de tus redes sociales para controlar quién puede ver y comentar tus publicaciones. Limita la información personal y evita la geolocalización automática.
- **Documentación y reporte del acoso:** Guarda capturas de pantalla, correos y mensajes de acoso como evidencia. Denuncia estas actividades a la plataforma correspondiente y, si es necesario, considera presentar una denuncia legal.

CAPÍTULO 1: COMPRENDIENDO LAS AMENAZAS DIGITALES PARA PERIODISTAS Y ACTIVISTAS

- **Estrategias para combatir la desinformación:** Si eres blanco de campañas de desinformación, utiliza tus redes sociales y contactos para aclarar la situación con hechos. Trabaja con organizaciones que luchen contra la desinformación para amplificar el mensaje correcto.

CALAS PÍTULO 2: PROTECCIÓN DE LA COMUNICACIÓN Y LAS FUENTES

Para periodistas y activistas, la comunicación segura y la protección de las fuentes son elementos críticos en su trabajo diario. Una comunicación filtrada o una fuente comprometida puede no solo poner en peligro una investigación, sino también poner en riesgo la vida de personas que confían en ti para denunciar injusticias y exponer verdades. Este capítulo explorará las mejores prácticas y herramientas disponibles para proteger tus conversaciones y mantener la confidencialidad de tus fuentes en un entorno digital cada vez más vulnerable.

2.1. Uso de Herramientas de Encriptación

La encriptación se ha convertido en una herramienta fundamental para mantener seguras tus comunicaciones. Asegura que, aunque un mensaje sea interceptado, solo el remitente y el destinatario puedan leerlo.

Cifrado de Correos Electrónicos. El correo electrónico sigue siendo una de las formas más comunes de comunicación, pero también es uno de los métodos más vulnerables si no se protegen adecuadamente. Aquí es donde entra en juego el cifrado.

CALAS PÍTULO 2: PROTECCIÓN DE LA COMUNICACIÓN Y LAS FUENTES

- **PGP (Pretty Good Privacy):** PGP es una herramienta popular que permite cifrar y descifrar correos electrónicos de manera segura. Funciona utilizando un par de claves: una clave pública (que se comparte con tus contactos para que cifren los mensajes que te envían) y una clave privada (que utilizas para descifrar los mensajes recibidos).

Cómo usar PGP:

- Instala un cliente de correo compatible: Thunderbird, con el complemento Enigmail, es una opción amigable y segura.
- Genera tu clave pública y privada: Esta clave te permitirá cifrar correos y enviarlos de forma segura.
- Verifica la identidad de tus contactos: Asegúrate de compartir tu clave pública de forma segura (preferiblemente en persona o mediante un canal confiable) para evitar ataques de intermediario.

- **Servicios de correo electrónico seguros:** Si prefieres una solución más sencilla, plataformas como ProtonMail y Tutanota ofrecen cifrado de extremo a extremo de manera integrada, lo que facilita el intercambio seguro de correos electrónicos sin configuraciones complicadas.

Mensajería Instantánea Cifrada. La mensajería instantánea se ha convertido en una herramienta rápida y efectiva para comunicarte con tus fuentes. Sin embargo, no todas las aplicaciones ofrecen el mismo nivel de seguridad.

- **Signal:** Es una de las aplicaciones más recomendadas para periodistas y activistas. Signal ofrece cifrado de extremo a extremo para mensajes, llamadas de voz y videollamadas. Además, es de código abierto, lo que permite auditorías de seguridad por parte de expertos independientes. También permite configurar mensajes que se autodestruyen después de un periodo determinado.
- **Wire:** Otra alternativa segura que ofrece cifrado de extremo a extremo y permite realizar llamadas y videollamadas seguras. Wire también es de código abierto y es una buena opción para quienes buscan una interfaz limpia y segura.

CAPÍTULO 2: SEGURIDAD DE LA INFORMACIÓN Y LA IMPORTANCIA DE LA DESTRUCCIÓN SEGURA

Consejos Prácticos para el Cifrado de Comunicación

- **Verifica la identidad de tus contactos:** Antes de intercambiar información sensible, verifica la identidad de la persona con la que te estás comunicando. En aplicaciones como Signal, puedes comparar las "huellas de seguridad" de tus contactos para garantizar que no hay un atacante en medio de la conversación.
- **Configura mensajes que se autodestruyen:** En aplicaciones como Signal y Wire, puedes habilitar la función de autodestrucción para que los mensajes se eliminen después de un cierto tiempo. Esto evita que las conversaciones se almacenen de forma indefinida y disminuye el riesgo de que sean descubiertas.
- **Mantén tus aplicaciones actualizadas:** Las actualizaciones suelen corregir fallas de seguridad, por lo que es fundamental que mantengas todas tus aplicaciones de comunicación actualizadas para protegerte de nuevas vulnerabilidades.

2.2. Anonimato en Línea

En muchos casos, mantener el anonimato en línea es fundamental para proteger tu identidad y la de tus fuentes. Tanto la navegación como la comunicación pueden dejar rastros que deben ocultarse para evitar compromisos.

Navegación Anónima y Protección de tu Identidad

- Tor Browser: Tor es un navegador que permite navegar por internet de forma anónima. Rutea tu tráfico a través de una red global de servidores, ocultando tu dirección IP y manteniendo tu actividad en línea privada. Es ideal para acceder a sitios web de forma segura y evitar rastreo.
    - Precauciones al usar Tor:
        - Evita ingresar información personal. Tor protege tu identidad, pero si ingresas datos personales en un sitio web, tu anonimato puede verse comprometido.

CAPÍTULO 2: SEGURIDAD DE LA INFORMACIÓN Y LA IMPORTANCIA DE LA DESTRUCCIÓN SEGURA

- **No instales complementos adicionales.** Las extensiones pueden exponer información privada o rastrear tu actividad.

- **VPN (Red Privada Virtual):** Una VPN oculta tu dirección IP al redirigir tu tráfico a través de un servidor seguro. Esto ayuda a proteger tu identidad y cifrar tu tráfico, especialmente al usar redes Wi-Fi públicas.
  - **Elegir una VPN confiable:**
    - **Sin registros de actividad:** Opta por un proveedor que no guarde registros de tu actividad en línea.
    - **Buena reputación de privacidad:** Investiga reseñas de usuarios y elige una VPN que sea confiable y transparente sobre su política de privacidad.

Uso de Sistemas Operativos Seguros

- **Tails OS:** Es un sistema operativo que se ejecuta desde una memoria USB, manteniendo tu actividad privada y anónima. Tails fuerza todo el tráfico a través de Tor y no deja rastros en el dispositivo utilizado.
- **Qubes OS:** Ofrece un enfoque más avanzado al aislar cada actividad (navegación, comunicación, trabajo) en máquinas virtuales separadas. Si una de estas máquinas virtuales se ve comprometida, no afectará al resto del sistema

Comunicación Anónima con Fuentes

- Cuentas desechables: Si necesitas comunicarte con una fuente de forma anónima, considera crear cuentas de correo electrónico y mensajería que no estén vinculadas a tu identidad.

CAPÍTULO 2: SEGURIDAD DE LA INFORMACIÓN Y LA IMPORTANCIA DE LA DESTRUCCIÓN SEGURA

- **Mensajería segura con anonimato:** Plataformas como Ricochet o Cwtch permiten comunicarte de forma anónima y descentralizada, sin servidores centrales que puedan registrar tu información.

2.3. Mantenimiento de la Confidencialidad de las Fuentes

La protección de tus fuentes es un aspecto crucial de la labor periodística y de activismo. Las fuentes confían en que su identidad y la información que comparten se mantendrán seguras, lo cual es vital para preservar su bienestar y confianza.

Uso de Plataformas de Confidencialidad

- **SecureDrop:** Una plataforma segura diseñada para recibir información sensible de fuentes de forma anónima. SecureDrop utiliza la red Tor para asegurar el anonimato tanto de las fuentes como del periodista, permitiendo el intercambio de archivos y mensajes de forma confidencial.
- **GlobaLeaks:** Una alternativa similar a SecureDrop, que facilita la recepción de información filtrada o denuncias de forma anónima y segura.

Protección de Documentos e Información Confidencial

- **Cifrado de documentos sensibles:** Almacena y comparte documentos confidenciales utilizando herramientas de cifrado de archivos, como VeraCrypt. Estas herramientas permiten cifrar carpetas completas y asegurar que solo quienes tengan la clave de acceso puedan acceder a la información.
- **Destrucción segura de información:** Cuando ya no necesites ciertos documentos o información, asegúrate de eliminarlos de forma segura. Usa software especializado que sobrescriba los archivos múltiples veces para asegurarte de que no puedan ser recuperados.

CAPÍTULO 3: SEGURIDAD EN DISPOSITIVOS Y ALMACENAMIENTO

Para periodistas y activistas, los dispositivos digitales como laptops, smartphones y tablets son herramientas fundamentales de trabajo. Estos dispositivos almacenan información confidencial, contactos de fuentes y proyectos sensibles. Sin embargo, también son vulnerables a una variedad de amenazas, desde accesos no autorizados hasta malware y pérdida de datos. Este capítulo aborda cómo proteger de manera efectiva tus dispositivos y garantizar que la información almacenada en ellos permanezca segura.

3.1. Protección de Laptops y Smartphones

La mayoría de las actividades diarias, como enviar correos electrónicos, redactar notas y comunicarse con fuentes, se realizan en laptops y smartphones. Por esta razón, es crucial implementar medidas de seguridad que aseguren que tu información esté protegida contra ataques y accesos no autorizados.

Configuraciones de Seguridad Básica

- Contraseñas fuertes y únicas: Elige contraseñas que sean difíciles de adivinar, combinando mayúsculas, minúsculas, números y símbolos. Evita usar contraseñas relacionadas con tu información personal, como nombres o fechas de cumpleaños, y evita reutilizarlas en diferentes cuentas.

CAPÍTULO 3: PROTECCIÓN DE MENSAJERÍA Y CONVERSACIONES PRIVADAS

- **Hackeos de mensajería:** Aplicaciones como WhatsApp y Telegram han sido objetivos constantes de ciberdelincuentes que buscan interceptar mensajes o tomar control de las cuentas. A pesar de que algunas de estas plataformas ofrecen cifrado de extremo a extremo, ningún sistema es completamente invulnerable si no se toman medidas de seguridad adicionales.

- **Autenticación biométrica:** Activa la autenticación biométrica (como huella digital o reconocimiento facial) para añadir una capa adicional de protección. Si bien la autenticación biométrica puede hacer que el acceso sea más conveniente, asegúrate de que esté combinada con un código de acceso seguro.

- **Bloqueo automático:** Configura el bloqueo automático en tus dispositivos después de un corto período de inactividad (por ejemplo, 1-2 minutos). Esto evitará que terceros accedan a tu dispositivo si lo dejas desatendido.

Cifrado de Dispositivos. El cifrado asegura que, en caso de robo o pérdida, la información almacenada en tu dispositivo no pueda ser accedida por terceros sin la contraseña de descifrado.

Cifrado de smartphones:

- **Android:** En dispositivos modernos, el cifrado suele estar activado de forma predeterminada. Puedes verificarlo en “Configuración” > “Seguridad” > “Cifrado y credenciales”.
- **iOS:** Todos los dispositivos Apple (iPhone, iPad) tienen cifrado de hardware habilitado automáticamente si el dispositivo está protegido con un código de acceso.

CAPÍTULO 3: PROTECCIÓN DE MENSAJERÍA Y CONVERSACIONES PRIVADAS

Cifrado de laptops:

- **Windows:** Usa BitLocker para cifrar el disco duro. BitLocker protege tu información almacenada y evita que sea accedida sin la contraseña de descifrado.
- **macOS:** Activa FileVault para cifrar el disco duro de tu Mac. FileVault asegura que los datos estén protegidos, incluso si el dispositivo cae en manos equivocadas.

Actualizaciones de Software y Parcheo Regular. Mantener el sistema operativo y las aplicaciones actualizadas es una de las formas más efectivas de protegerte contra vulnerabilidades conocidas.

Automatiza las actualizaciones: Configura tus dispositivos para que instalen actualizaciones automáticamente. Las actualizaciones de seguridad corrigen fallas que podrían ser explotadas por atacantes.

- **Verifica la fuente de las aplicaciones:** Instala aplicaciones únicamente de fuentes confiables, como la tienda oficial de tu dispositivo (Google Play Store o Apple App Store). Las aplicaciones descargadas de sitios web de terceros pueden contener malware.

3.2. Destrucción Segura de Información y Almacenamiento Seguro

Los periodistas y activistas trabajan con información sensible que puede ser peligrosa si cae en manos equivocadas. Es importante no solo proteger la información mientras está en uso, sino también asegurarse de que, cuando ya no sea necesaria, se elimine de manera segura.

Almacenamiento Seguro de Información

- **Uso de cifrado de archivos y carpetas:** Para documentos o carpetas

CAPÍTULO 3: PROTECCIÓN DE MENSAJERÍA Y CONVERSACIONES PRIVADAS

específicas que contienen información sensible, utiliza herramientas de cifrado adicionales como VeraCrypt. Este software de código abierto permite cifrar carpetas y particiones de disco con contraseñas fuertes, asegurando que solo personas autorizadas puedan acceder a los datos.

- **Backup seguro de datos:** Realiza copias de seguridad de tu información de manera regular. Asegúrate de que estos backups estén almacenados de forma segura, ya sea en un disco duro cifrado o en un servicio de almacenamiento en la nube que ofrezca cifrado de extremo a extremo.

Destrucción Segura de Información Digital.Simplemente borrar un archivo o carpeta no es suficiente para asegurar que la información haya sido eliminada. La mayoría de los sistemas operativos simplemente marcan los archivos como "eliminados" y su contenido sigue estando presente en el disco hasta que se sobrescriba.

- **Software de borrado seguro:** Usa herramientas que sobrescriben los archivos múltiples veces para que no puedan ser recuperados. Algunas opciones recomendadas son Eraser (para Windows) y BleachBit (para Windows, macOS y Linux). Estos programas garantizan que, al eliminar un archivo, sus datos sean sobrescritos y destruidos permanentemente.
- **Eliminación de discos duros:** Si necesitas eliminar un disco duro o unidad externa, es recomendable realizar un borrado seguro de la unidad completa antes de desecharla. Algunos programas de borrado seguro permiten eliminar datos de todo el disco de manera irreversible.

CAPÍTULO 3: PROTECCIÓN DE MENSAJERÍA Y CONVERSACIONES PRIVADAS

Destrucción Física de Dispositivos. En casos en los que la información almacenada en un dispositivo es extremadamente sensible y no debe ser accesible bajo ninguna circunstancia, la destrucción física es la opción más segura.

- **Destrucción de discos duros y SSDs:**
  - **Desmagnetización:** Si es posible, usa un desmagnetizador industrial para borrar los datos almacenados en discos duros mecánicos.
  - **Trituración o perforación:** Para discos duros mecánicos y unidades SSD, la trituración o perforación física del disco es una opción efectiva para garantizar que los datos no puedan ser recuperados.

- **Destrucción de medios extraíbles:**
  - **CDs/DVDs:** Corta los discos en varias piezas para evitar que sean leídos nuevamente.
  - **USBs y tarjetas SD:** Tritura o corta físicamente las unidades para destruir la memoria interna.

3.3. Protección de Dispositivos Contra el Acceso Físico No Autorizado

Aunque proteger los dispositivos digitalmente es crucial, también es importante evitar que otras personas tengan acceso físico a ellos.

CAPÍTULO 3: PROTECCIÓN DE MENSAJERÍA Y CONVERSACIONES PRIVADAS

Seguridad Física en el Uso Diario

- **Uso de candados de seguridad para laptops:** Si trabajas en espacios públicos o de coworking, utiliza candados de seguridad para evitar el robo de tu laptop. Estos candados se aseguran a la computadora y a una superficie fija.
- **Supervisión constante de dispositivos móviles:** Mantén tus dispositivos siempre a la vista y no los dejes desatendidos, especialmente en lugares públicos. Si necesitas dejarlos por un momento, guárdalos en un lugar seguro o pide a un colega de confianza que los supervise.

Almacenamiento Seguro de Dispositivos Fuera de Uso

- **Cajas fuertes o armarios cerrados:** Cuando no uses tu laptop, tablet o smartphone, guárdalos en una caja fuerte o armario cerrado con llave. Esto previene accesos no autorizados y evita que sean robados.
- **Protección de documentos físicos:** Si tienes notas, documentos impresos u otros materiales físicos confidenciales, almacénalos en archivadores seguros o cajas fuertes.

Tus dispositivos digitales son portales a tu información más confidencial, y protegerlos es fundamental para mantener tu seguridad y la de tus fuentes. Asegúrate de aplicar medidas como el cifrado, el uso de contraseñas fuertes y la eliminación segura de información para proteger tus datos. Y no olvides que la seguridad no solo es digital; proteger tus dispositivos físicamente también es esencial.

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

La navegación por internet es parte fundamental del trabajo de periodistas y activistas, ya sea para investigar, comunicarse o compartir información. Sin embargo, cada vez que te conectas, dejas un rastro de tu actividad, ubicaciones y datos personales que pueden ser explotados por actores maliciosos. En este capítulo, aprenderás cómo navegar de forma segura y proteger tu privacidad en línea para evitar el rastreo, la exposición de datos y la manipulación de tu actividad en internet.

4.1. Uso de VPNs y Navegación Anónima

Una Red Privada Virtual (VPN) es una herramienta clave para proteger tu actividad en línea. Las VPNs cifran tu tráfico de internet y lo redirigen a través de un servidor seguro, ocultando tu dirección IP real y protegiendo tu identidad.

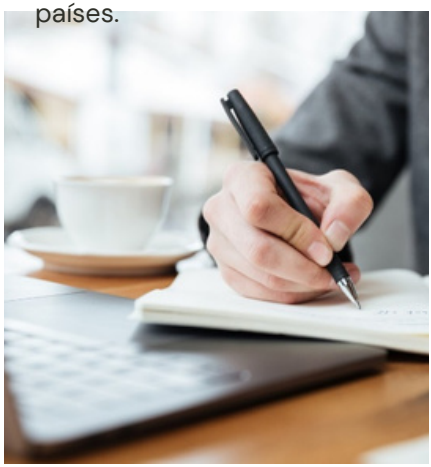
Beneficios de Usar una VPN

- **Protección de tu identidad y privacidad:** Al ocultar tu dirección IP, la VPN te permite navegar por internet de forma anónima y evita que tu proveedor de servicios de internet (ISP) u otros actores puedan rastrear tu actividad en línea.
- **Conexiones seguras en redes públicas:** Si trabajas desde un café, hotel o cualquier otra red Wi-Fi pública, tu tráfico puede ser

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

interceptado fácilmente por atacantes. Usar una VPN en redes públicas cifra tus datos y los protege contra intentos de espionaje y ataques de intermediario (Man-in-the-Middle).

- **Acceso a contenido restringido:** En países donde ciertos sitios web o servicios están bloqueados, una VPN puede ayudarte a acceder a estos contenidos al conectarte a través de servidores en otros países.



Cómo Elegir una VPN Confiable

- **Política de no registros (no-logs policy):** Elige un proveedor de VPN que no almacene registros de tu actividad en línea. Esto garantiza que, incluso si el proveedor de VPN es atacado o requerido por autoridades, no tendrá información para compartir sobre tu actividad.
- **Cifrado fuerte y protocolos seguros:** Busca VPNs que utilicen protocolos de cifrado fuertes, como OpenVPN o WireGuard. Estos protocolos son conocidos por su seguridad y eficiencia.
- **Jurisdicción favorable a la privacidad:** Considera la ubicación del proveedor de VPN. Algunos países tienen leyes de vigilancia más estrictas, lo que puede hacer que tu privacidad esté en riesgo. Opta por VPNs ubicadas en países con una fuerte protección de la privacidad, como Suiza o Islandia.

VPNs Recomendadas para la Seguridad y Privacidad

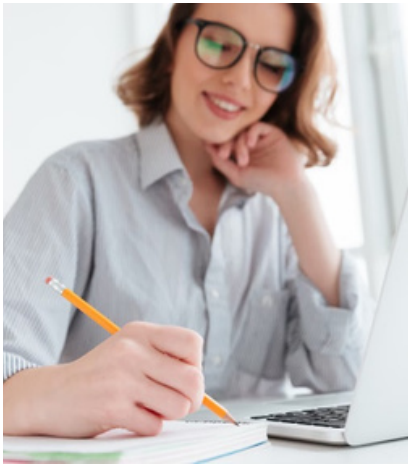
- **NordVPN:** Ofrece una fuerte política de privacidad, cifrado avanzado y una red de servidores en múltiples países.
- **ExpressVPN:** Conocida por su velocidad, seguridad y facilidad de uso, además de una sólida política de no registros.
- **ProtonVPN:** Gestionada por la misma empresa detrás de ProtonMail, ofrece altos estándares de seguridad y privacidad, con enfoque en la protección de derechos digitales.

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

Precauciones al Usar una VPN

- **Habilita el "Kill Switch":** La mayoría de las VPNs tienen una función llamada "Kill Switch" que bloquea el acceso a internet si la conexión con la VPN se pierde. Esto evita que tu tráfico quede expuesto accidentalmente.
- **Evita VPNs gratuitas:** Las VPNs gratuitas pueden monetizar tu tráfico vendiendo tus datos a terceros o insertando anuncios en tu navegación. Si bien son convenientes, pueden representar un riesgo para tu privacidad.

4.2. Navegación Segura con Tor y Navegadores Privados



En situaciones donde el anonimato es fundamental, el uso de navegadores especializados puede ofrecer un nivel extra de privacidad.

Tor Browser: El Navegador para la Anonimización Total El Tor Browser es un navegador que te permite navegar por internet de manera anónima al redirigir tu tráfico a través de una red de nodos (servidores) distribuidos por todo el mundo. Esta técnica oculta tu dirección IP y hace muy difícil rastrear tu actividad en línea.

Uso de Navegadores Privados y Extensiones de Seguridad

- **Firefox con extensiones de privacidad:** Firefox es un navegador que ofrece varias opciones para mejorar la privacidad. Combínalo con extensiones como uBlock Origin (para bloquear rastreadores y anuncios), HTTPS Everywhere (para asegurar que tu conexión con sitios web sea cifrada) y Privacy Badger (para bloquear rastreadores de terceros).
- **Brave Browser:** Brave es un navegador enfocado en la privacidad que

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

bloquea automáticamente rastreadores, anuncios y cookies de terceros. Además, ofrece la opción de navegar con Tor directamente desde el navegador para un mayor nivel de anonimato.

4.3. Precauciones en Redes Sociales y Control de tu Huella Digital

Las redes sociales son herramientas esenciales para difundir información y construir una red de contactos, pero también pueden poner en riesgo tu privacidad y exponer datos sensibles si no se gestionan adecuadamente.

Configuraciones de Privacidad en Redes Sociales

- **Revisa y ajusta la privacidad de tus perfiles:** Configura quién puede ver tus publicaciones, fotos e información de perfil. Limita la visibilidad a “solo amigos” o “solo contactos de confianza” en lugar de hacerlo público.
- **Controla la geolocalización:** Desactiva la función de geolocalización en redes sociales para evitar que tus publicaciones incluyan información sobre tu ubicación actual. Compartir tu ubicación en tiempo real puede exponer tu rutina y ponerte en riesgo.
- **Configura alertas de inicio de sesión:** Activa alertas para recibir notificaciones sobre intentos de inicio de sesión desde ubicaciones desconocidas o dispositivos nuevos. Esto te permitirá identificar posibles intentos de hackeo rápidamente.

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

Publicaciones Seguras y Cuidado con el Contenido que Compartes

- **No compartas información sensible:** Evita publicar datos personales como direcciones, números de teléfono, horarios de trabajo, o información que pueda ser utilizada para identificarte o localizarte.

- **Cuidado con fotos y metadatos:** Las fotos que publicas pueden contener metadatos (información sobre la ubicación y el dispositivo utilizado para capturarlas). Antes de compartir una imagen, usa herramientas para eliminar estos metadatos o configura tu dispositivo para que no los incluya.

Gestión de Solicitudes de Amistad y Seguidores

- Verifica contactos nuevos: Antes de aceptar una solicitud de amistad o conexión, verifica que el perfil sea genuino. Los atacantes pueden crear perfiles falsos para obtener información sobre ti o ganarse tu confianza.
- Sé selectivo con tus conexiones: No aceptes solicitudes de personas que no conozcas o que no hayan sido verificadas por alguien de confianza.

4.4. Medidas Adicionales de Seguridad para Navegación y Conexiones en Línea

Uso de DNS Seguros y Bloqueadores de Rastreo

- **DNS seguro:** Un DNS (Domain Name System) es el sistema que traduce las direcciones web (como www.ejemplo.com) a direcciones IP. Utiliza servicios de DNS seguros como Cloudflare DNS (1.1.1.1) o Google DNS (8.8.8.8) para mejorar la privacidad y evitar ataques como el phishing.
- **Bloqueadores de rastreadores y anuncios:** Herramientas como uBlock Origin o AdGuard ayudan a bloquear rastreadores y anuncios que pueden recopilar información sobre tu actividad en línea.

CAPÍTULO 4: NAVEGACIÓN SEGURA Y PROTECCIÓN EN LÍNEA

Protección contra Ataques de Intermediario (Man-in-the-Middle)

- **Conexión a través de HTTPS:** Asegúrate de que todos los sitios web que visitas utilizan HTTPS (en lugar de HTTP) para cifrar la conexión entre tu dispositivo y el sitio web. Instala la extensión HTTPS Everywhere para forzar automáticamente conexiones seguras cuando sea posible.
- **Evita redes Wi-Fi abiertas y sin cifrar:** Las redes Wi-Fi públicas sin cifrado (como las que no requieren contraseña) son un caldo de cultivo para ataques de intermediario. Si es necesario conectarse a una red pública, usa una VPN para proteger tu tráfico.

La forma en que navegas por internet puede tener un impacto significativo en tu privacidad y seguridad. Utiliza herramientas como VPNs y navegadores seguros para proteger tu identidad, ajusta la configuración de privacidad en redes sociales para controlar quién ve tu información, y asegúrate de que todas tus conexiones sean cifradas. Mantener tu actividad en línea protegida es clave para preservar tu seguridad digital.

CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

En el trabajo de periodistas y activistas, la posibilidad de enfrentarse a incidentes de seguridad digital es real y constante. Sin embargo, contar con un plan de respuesta puede marcar la diferencia entre mitigar rápidamente el daño o sufrir consecuencias graves. En este capítulo, exploraremos cómo identificar señales de ataque, cómo actuar de manera inmediata ante un incidente y cómo prepararte para posibles amenazas futuras a través de un plan sólido de respuesta.

5.1. Identificación de Señales de Ataque

Saber reconocer los signos de un posible ataque cibernético es el primer paso para proteger tus datos y responder a tiempo.

Comportamientos Anómalos en Dispositivos

- **Rendimiento inusualmente lento:** Si tu computadora o smartphone se vuelve repentinamente más lento sin razón aparente, podría estar siendo utilizado para actividades no autorizadas (como minería de criptomonedas o envío de datos a un atacante).
- **Batería que se agota rápidamente:** Un dispositivo que presenta un agotamiento de batería repentino podría estar ejecutando procesos ocultos, como spyware o aplicaciones maliciosas en segundo plano.

CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

- **Aumento inesperado en el uso de datos móviles:** Un aumento significativo en el tráfico de datos sin que tú lo hayas provocado puede ser una señal de que tu dispositivo está enviando información a un servidor remoto de forma no autorizada.
- **Comportamiento errático:** Ventanas emergentes, aplicaciones que se abren o cierran solas, y configuraciones que cambian sin tu autorización pueden indicar la presencia de malware.

Alertas de Seguridad en Cuentas y Servicios

- Intentos de inicio de sesión sospechosos: Las notificaciones de inicio de sesión desde ubicaciones desconocidas o dispositivos no reconocidos pueden ser un indicio de que alguien está intentando acceder a tu cuenta.
- Cambios inesperados en contraseñas o configuraciones: Si recibes alertas de cambios de contraseñas o configuraciones de cuenta que no realizaste, actúa de inmediato para asegurar tu cuenta.

Comunicación Sospechosa

- **Mensajes extraños de tus contactos:** Si amigos o colegas te envían mensajes informándote de correos o mensajes extraños enviados desde tus cuentas, podría significar que tu cuenta ha sido comprometida y está siendo utilizada para enviar spam o phishing.

5.2. Pasos a Seguir en Caso de Compromiso

Si identificas alguna señal de posible compromiso, actúa rápidamente para minimizar el daño y proteger tu información.

CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

Desconexión Inmediata de Dispositivos Comprometidos

- **Desconecta de internet:** Si sospechas que tu dispositivo ha sido comprometido, desconéctalo de cualquier red de internet (Wi-Fi, datos móviles) para detener la transmisión de datos y prevenir que el atacante tenga más acceso.
- **Apaga conexiones inalámbricas:** Deshabilita Wi-Fi, Bluetooth y cualquier otra conexión inalámbrica en tu dispositivo para evitar que sigan transmitiendo datos.

Cambio de Contraseñas y Control de Acceso a Cuentas

- **Desde un dispositivo seguro:** Utiliza un dispositivo confiable (que no esté comprometido) para cambiar todas las contraseñas de tus cuentas importantes, como correo electrónico, redes sociales, aplicaciones bancarias y servicios de almacenamiento en la nube.
- **Prioriza cuentas críticas:** Comienza con aquellas cuentas que puedan tener el mayor impacto si se ven comprometidas, como correo electrónico principal, banca en línea y redes sociales profesionales.

Análisis y Limpieza del Dispositivo Comprometido

- **Usa software de seguridad:** Realiza un escaneo completo de tu dispositivo con software antivirus y antimalware actualizado. Si la herramienta detecta amenazas, sigue los pasos recomendados para eliminarlas.
- **Restablecimiento de fábrica:** Si sospechas que tu dispositivo ha sido severamente comprometido y no puedes eliminar las amenazas, considera realizar un restablecimiento de fábrica. Esto eliminará todos los datos y configuraciones del dispositivo, pero asegúrate de hacer una copia de seguridad de tus datos importantes (cifrados y en un dispositivo seguro) antes de proceder.

Notificación a Contactos y Fuentes

- **Informa sobre el compromiso:** Si tu cuenta ha sido hackeada, notifica a tus contactos para que no abran mensajes sospechosos enviados desde tu cuenta. Esto es especialmente importante si manejas información confidencial de tus fuentes.

CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

5.3. Preparación y Plan de Respuesta a Incidentes Futuros

Tener un plan de respuesta a incidentes te permitirá actuar rápida y eficazmente si ocurre un ataque. La preparación es clave para proteger tus activos digitales y minimizar el impacto de una brecha de seguridad.

Creación de un Plan de Respuesta a Incidentes
Definir roles y responsabilidades: Si trabajas en un equipo, asigna responsabilidades claras para la respuesta a incidentes. Define quién será responsable de cambiar contraseñas, quién notificará a las partes afectadas y quién tomará el control de los dispositivos comprometidos.

- **Documenta los procedimientos:** Crea una guía paso a paso para responder a diferentes tipos de incidentes, como ataques de phishing, hackeo de cuentas o infección por malware. Asegúrate de que esta guía esté accesible para todos los miembros del equipo.

Respaldo y Recuperación de Datos

- **Realiza copias de seguridad frecuentes:** Crea backups regulares de tus datos importantes en medios seguros, como discos duros cifrados o servicios de almacenamiento en la nube con cifrado. Asegúrate de que los backups estén desconectados de la red cuando no se estén usando para evitar su compromiso.
- **Plan de restauración de datos:** Verifica que puedas restaurar tus datos rápidamente desde las copias de seguridad si es necesario. Realiza pruebas periódicas para asegurarte de que los backups funcionan correctamente.

CAPÍTULO 5: PREPARACIÓN ANTE INCIDENTES Y PLAN DE RESPUESTA

Revisión y Mejora Continua de Seguridad

- **Lecciones aprendidas:** Después de resolver un incidente, realiza una revisión detallada para entender cómo ocurrió el ataque y qué medidas pueden implementarse para prevenir futuros eventos.
- **Mantén una cultura de seguridad activa:** Capacítate y capacita a todos los miembros de tu equipo sobre buenas prácticas de seguridad digital y actualiza regularmente tus protocolos de respuesta a incidentes.

CONCLUSIÓN

"PROTEGE TU MISIÓN, PROTEGE TU VOZ. LA SEGURIDAD DIGITAL ES LA CLAVE PARA QUE TU VERDAD SEA ESCUCHADA."

La labor de periodistas y activistas es fundamental para la sociedad, pero también conlleva riesgos digitales únicos y complejos. Al proteger tu identidad, comunicaciones y dispositivos, puedes continuar realizando tu trabajo de manera segura y efectiva, evitando que las amenazas cibernéticas interfieran con tu misión y objetivos.

A través de este e-book, hemos explorado cómo proteger tu información en todos los aspectos de tu actividad digital, desde el uso seguro de dispositivos hasta la navegación por internet, la comunicación con fuentes y la respuesta efectiva ante incidentes de seguridad.

La seguridad digital es un proceso continuo que requiere atención y actualización constante. Recuerda que no solo estás protegiendo tu información, sino también la de tus fuentes, contactos y comunidades que dependen de tu labor.

AGRADECIMIENTOS

Queremos expresar nuestro más sincero agradecimiento a todas las personas que han contribuido a la creación de este e-book. A los periodistas y activistas que día a día se enfrentan a desafíos digitales para proteger y comunicar la verdad, gracias por inspirarnos a desarrollar esta guía. Esperamos que los consejos y recursos aquí presentados sean de utilidad para fortalecer su seguridad y continuar con su valiosa labor.

Un agradecimiento especial a cada lector que ha dedicado su tiempo para explorar estas páginas. Sabemos que la seguridad digital puede parecer un tema técnico y complejo, pero confiamos en que este e-book haya simplificado los conceptos y herramientas necesarios para proteger tu información y tu misión.

Gracias por confiar en nosotros como tu aliado en ciberseguridad y seguridad de la información. Juntos, estamos construyendo un entorno digital más seguro y protegido para quienes trabajan por la justicia, la transparencia y la defensa de los derechos humanos.

Contáctanos dando clic en este botón:

CONTACTANOS

Gracias

Escanéame

contacto@templarciberseguridad.com
www.templarciberseguridad.com
+57 3054594430

contacto@templarciberseguridad.com
www.templarciberseguridad.com
+57 3054594430