Manual de seguridad digital para organizaciones sociales y de derechos humanos

Luis Ángel Saavedra Mendoza

Serie Capacitación # 45

INREDH

Fundación Regional de Asesoría en Derechos Humanos
INREDH

Manual de seguridad digital para organizaciones sociales y de derechos humanos

Quito, junio de 2024

Manual de seguridad digital para organizaciones sociales y de derechos humanos

Serie Capacitación # 45

Editora: Verónica Yuquilema Yupangui
Presidenta INREDH
Autor: Luis Ángel Saavedra Mendoza

Fundación Regional de Asesoría en Derechos Humanos, INREDH
Av. 10 de Agosto N34 - 80 y Rumipamba - Piso 1 - Quito, Ecuador
Telefax: 593 2 2446970
Correo: info@inredh.org
Web: www.inredh.org

ISBN: 978-9978-980-66-8

Primera **edición: junio** de 2024
Edición y diagramación: Puento Digital
Fotografía: archivo INREDH
Impresión: EcoPrint

El Presente manual fue realizado por INREDH, con el apoyo de la Fundación Nacional para la Democracia, NED.

ÍNDICE

1. LA SEGURIDAD DIGITAL PARAORGANIZACIONES DEFENSORAS DE DERECHOS HUMANOS

a. Introducción

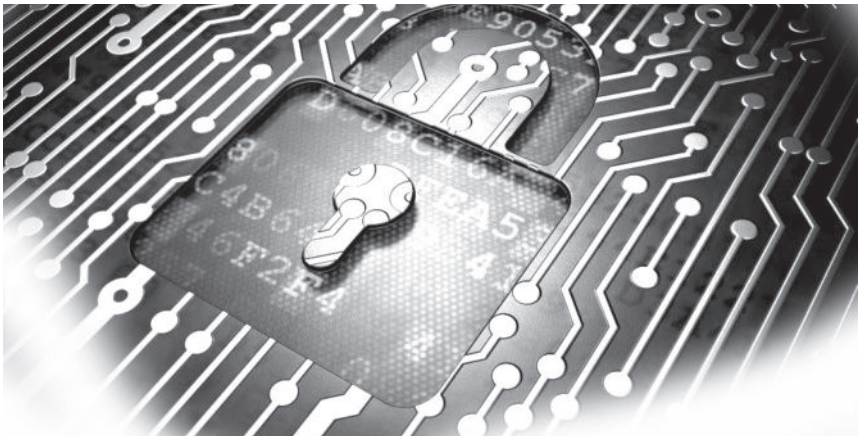
En un mundo cada vez más digitalizado, la protección de la información se ha convertido en un tema fundamental para las organizaciones sociales y de derechos humanos. La capacidad de comunicarse de manera segura, almacenar y proteger datos sensibles, salvaguardar la privacidad de las personas que integran el equipo de trabajo, víctimas o beneficiaros son elementos importantes para garantizar la efectividad y la seguridad de estas organizaciones. Este manual de seguridad digital está diseñado para ayudar a organizaciones sociales, de derechos humanos, activistas y comunicadores a fortalecer sus prácticas de seguridad cibernética y protegerse de amenazas que podrían comprometer su trabajo vital en la defensa de los derechos humanos. A lo largo de estas páginas, exploraremos desde principios básicos de la seguridad digital, las amenazas e incidentes de seguridad y una recopilación de varias herramientas prácticas y consejos para mitigar riesgos y fortalecer la seguridad digital de las organizaciones sociales y de derechos humanos.

b. Importancia de la seguridad digital para organizaciones de derechos humanos

En un contexto global donde la información sensible y estratégica está constantemente en riesgo. Las organizaciones sociales y de derechos humanos manejan datos sensibles relacionados con individuos en

situaciones vulnerables, activistas, acciones, proyectos o información que requiere protección y seguridad digital contra ciber ataques, suplantación de identidad, vigilancia continua, ataque DDoS, entre otras formas que buscan vulnerar la seguridad de las organizaciones.

Por lo que se puede afirmar que la seguridad digital no solo resguarda la integridad y la confidencialidad de los datos, sino que también preserva la credibilidad y la efectividad de las acciones emprendidas en la defensa de los derechos humanos. El establecer un plan de seguridad digital en las organizaciones, es garantizar la protección integral de quienes confían en la organización, así como de sus colaboradores quienes por su labor a menudo se encuentran en riesgos físicos y digitales.



c. Conceptos Básicos de seguridad digital

Algunos de los conceptos básicos en seguridad digital refieren a:

La **confidencialidad,** por ejemplo, asegura que solo las personas autorizadas puedan acceder a la información. Para lograrlo, las organizaciones pueden utilizar el cifrado de datos en sus dispositivos de trabajo o en comunicaciones sensibles como correos electrónicos y documentos almacenados en la nube. Además, se sugiere que se implementen políticas estrictas de acceso y autenticación mediante el uso de contraseñas fuertes y sistemas de autenticación en dos pasos.

Los **respaldos de información** aseguran que la información no se pierda y esté disponible cuando se los necesite. Se sugiere que las organizaciones sociales y de derechos humanos utilicen sistemas de respaldo de manera frecuente para asegurar que los datos sensibles estén disponibles en caso de fallas en el sistema principal o ataques que intenten vulnerar a los servidores. Los respaldos de información nos permiten darles continuidad a los proyectos y actividades incluso en situaciones de emergencia, como ataques cibernéticos, robo de información, contextos de conmoción social y desastres naturales.

Desde nuestra experiencia hemos identificado que la **gestión de contraseñas** en las organizaciones sociales, no es la más adecuada, desde su creación se utiliza contraseñas fáciles de recordar relacionadas a fechas de cumpleaños o contraseñas numéricas simples como 1234: pero además se ha observado que las contraseñas de los perfiles de redes sociales, correos o incluso administradores de sitios web son compartidas por medio de aplicaciones de mensajería instantánea como Whatsapp o Telegram, lo cual podría significar una vulnerabilidad digital para las organizaciones.

Para llevar un control sobre estos factores se sugiere a las organizaciones sociales y de derechos humanos implementar un plan de acción y prevención en seguridad digital; en el cual se establezca una periodicidad para realizar respaldos y cambio de contraseñas o incluso pasos a seguir en caso de incidentes como la perdida de información o suplantación de la identidad; en el contexto del labor periodístico, a este ejercicio las Naciones Unidas lo definen como "Una amplia categoría que engloba desde medidas preventivas y protectoras en seguridad que abarca el ámbito tanto online como offline, y […] las soluciones requieren de acciones informadas a nivel global, nacional y local, al tiempo que se responde a especificidades contextuales en cada caso". (Henrichsen, J. R., Betz, M., & Lisosky, J. M. 2016)

2. AMENAZAS COMUNES PARA ORGANIZACIONES DE DERECHOS HUMANOS

Las organizaciones sociales, de derechos humanos, así como activistas y comunicadores se enfrentan a diversas amenazas cibernéticas que pueden comprometer la seguridad de la información sensible que manejan. (Aycardi, G. A. R., & Joseph, P. 2017).
Algunas de las amenazas que hemos identificado son:

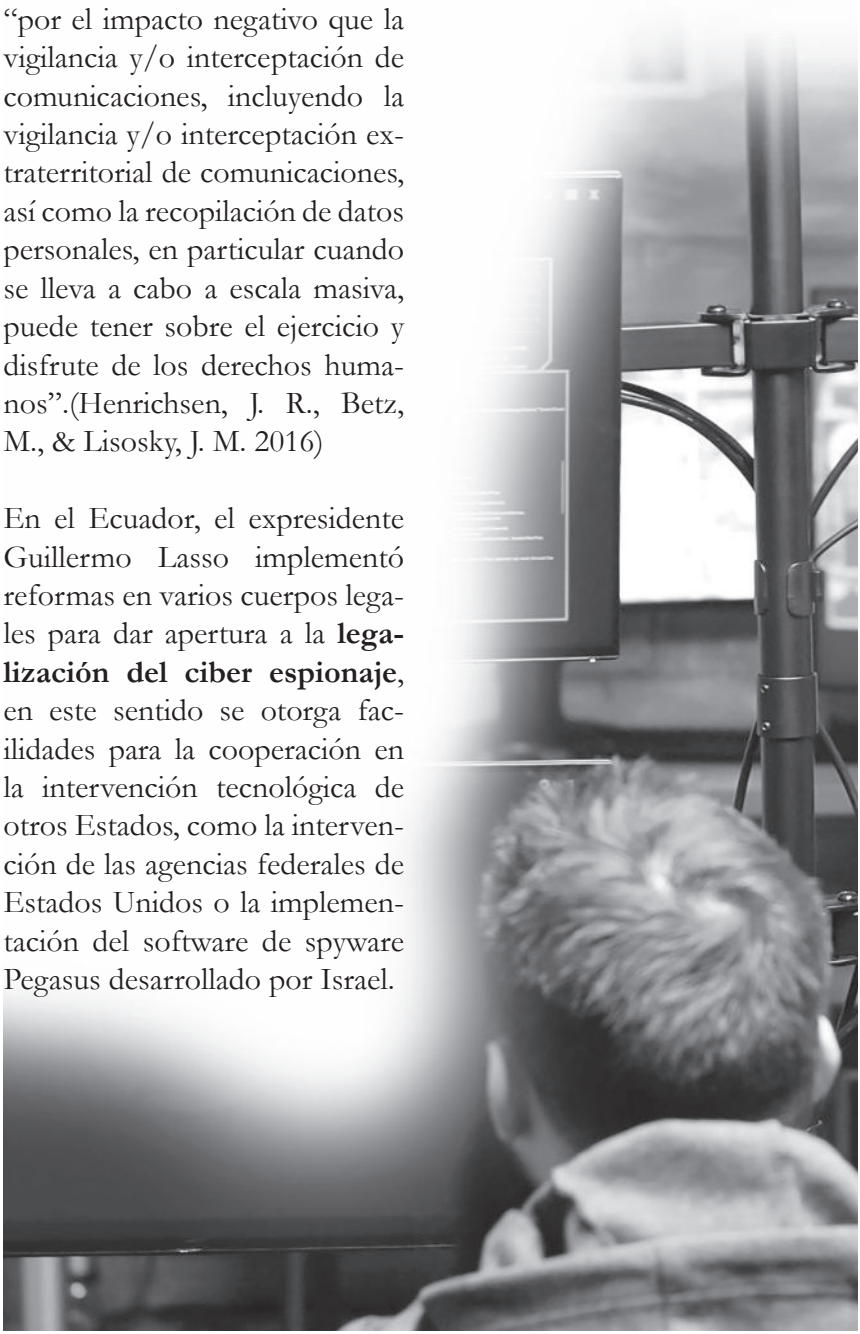
a. Vigilancia y vigilancia masiva

La vigilancia puede producirse de forma masiva o estar dirigida a individuos.

Cuando la vigilancia se recopila de manera masiva y está "no cuenta con una supervisión fiable por parte de un organismo independiente de monitoreo, puede menoscabar derechos humanos –incluyendo la libertad de expresión, la libertad de asociación y el derecho a la privacidad– y **amenazar a la democracia**. Esto está reconocido en una resolución del Consejo de Derechos Humanos adoptada en marzo de 2014, donde se regis-

tró una profunda preocupación "por el impacto negativo que la vigilancia y/o interceptación de comunicaciones, incluyendo la vigilancia y/o interceptación extraterritorial de comunicaciones, así como la recopilación de datos personales, en particular cuando se lleva a cabo a escala masiva, puede tener sobre el ejercicio y disfrute de los derechos humanos".(Henrichsen, J. R., Betz, M., & Lisosky, J. M. 2016)

En el Ecuador, el expresidente Guillermo Lasso implementó reformas en varios cuerpos legales para dar apertura a la **legalización del ciber espionaje**, en este sentido se otorga facilidades para la cooperación en la intervención tecnológica de otros Estados, como la intervención de las agencias federales de Estados Unidos o la implementación del software de spyware Pegasus desarrollado por Israel.



En la administración del actual presidente Daniel Noboa, **se usó al Centro de Inteligencia Estratégica** para vigilar a la periodista Alondra Santiago, organismo que después emitió un informe donde considera a la periodista como una amenaza para la seguridad nacional; Alondra Santiago tuvo que salir del país para proteger su integridad física, no obstante, este hecho es el más reciente donde se utiliza la vigilancia y en concreto a un organismo que realiza ciber espionaje para perseguir a quienes son críticos del gobierno; dicho lo cual se vulnera el derecho a la libertad de expresión.

b. Exploits de software y hardware sin el conocimiento del individuo objetivo

La tecnología de vigilancia puede también utilizarse para i**nfectar computadoras** en todo el mundo con "implantes" de malware que permiten a entidades externas introducirse en redes informáticas específicas. Llamamos "Malware" a los tipos de software y programas maliciosos que afectan de distintas maneras los dispositivos.

Algunos de los tipos más comunes de malware son:

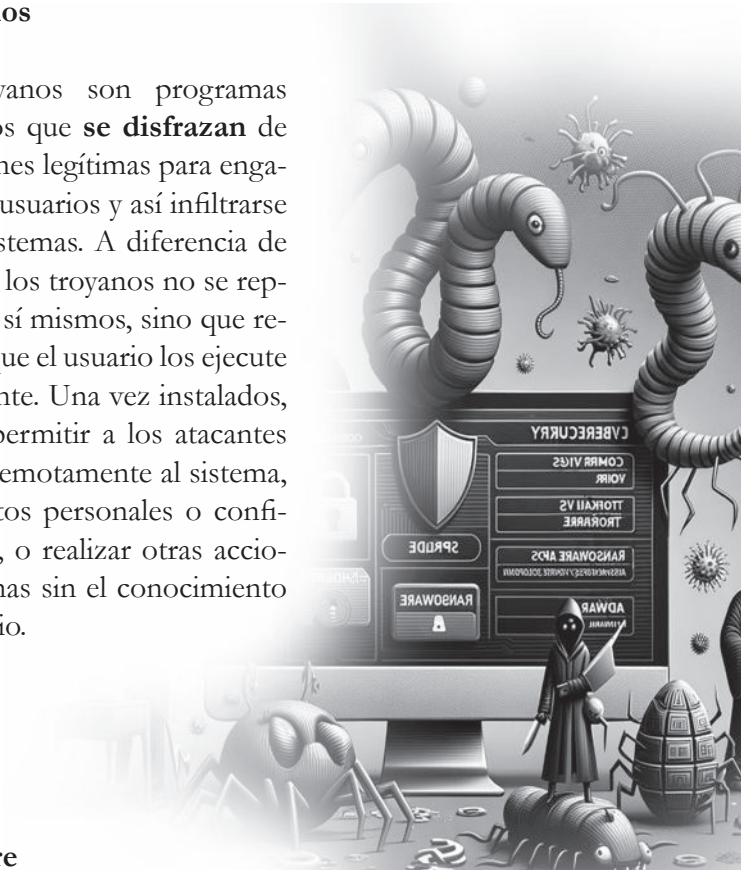
• Virus informático

Un virus informático es un programa o código malicioso diseñado para replicarse y propagarse entre archivos y sistemas informáticos. Su objetivo principal es **causar daño al sistema**, ya sea corrompiendo datos, eliminando archivos o afectando el rendimiento general de la computadora. Los virus suelen propagarse aprovechando vulnerabilidades en el software o

a través de acciones del usuario como la descarga de archivos infectados.

• Troyanos

Los troyanos son programas maliciosos que **se disfrazan** de aplicaciones legítimas para engañar a los usuarios y así infiltrarse en sus sistemas. A diferencia de los virus, los troyanos no se replican por sí mismos, sino que requieren que el usuario los ejecute activamente. Una vez instalados, pueden permitir a los atacantes acceder remotamente al sistema, robar datos personales o confidenciales, o realizar otras acciones dañinas sin el conocimiento del usuario.



• Spyware

El spyware es un tipo de software malicioso diseñado para **recopilar información** sobre las actividades de los usuarios en sus dispositivos, sin su consentimiento. Suele ser utilizado para espiar hábitos de navegación, robar contraseñas, registrar pulsaciones de teclado u obtener datos personales con fines fraudulentos. El spyware suele ser instalado inadvertidamente junto con software aparentemente legítimo o a través de descargas en línea.

• **Gusanos**

Los gusanos son programas informáticos que se propagan de manera autónoma a través de redes informáticas y sistemas conectados, sin necesidad de intervención humana directa. A diferencia de los virus, los gusanos no necesitan infectar archivos específicos, sino que aprovechan vulnerabilidades de red para **replicarse y distribuirse** rápidamente. Pueden causar congestión en redes, ralentización de sistemas y pérdida de datos.

• **Ransomware**

El ransomware es un tipo de malware que **restringe el acceso** a los archivos o sistemas de una víctima y exige el pago de un rescate para restaurar el acceso. Suele cifrar archivos importantes o bloquear completamente el acceso al sistema, dejando a los usuarios incapaces de utilizar sus dispositivos hasta que paguen la suma exigida. Los ransomware pueden propagarse a través de correos electrónicos maliciosos, descargas de software infectado o vulnerabilidades de red.

c. Ataques de phishing

Un ataque de phishing es cuando **alguien intenta engañarte** para que reveles información personal o confidencial, como contraseñas, números de tarjetas de crédito o detalles de cuentas bancarias. Usualmente lo hacen enviando correos electrónicos o mensajes falsos que parecen venir de empresas legítimas, como bancos o tiendas en línea. El objetivo es que hagas clic en enlaces maliciosos o descargues archivos infectados

Cuando los ataques de phishing son **dirigidos hacia organizaciones o comunicadores**, a menudo utilizan enlaces o archivos adjuntos cargados con malware que son enviados a través de e-mail o redes sociales. Aunque el malware difiere en sus capacidades, una de las maneras más malévolas que se ha sabido que afecta la labor de comunicadores

y personas defensoras de derechos humanos son los Troyanos de Acceso Remoto (RAT). Entre más sofisticado es un RAT, más probable es que evite la detección por parte de un antivirus. Si se hace clic sobre ellos o son descargados, estos RAT permiten al atacante recopilar cualquier cosa que quieran en el dispositivo comprometido.

d. Ataques de intermediario o man-in-the-middle (MitM)

Un ataque de intermediario, también conocido como "man-in-the-middle" (MitM), ocurre cuando un **hacker se mete** en medio de la comunicación entre dos partes que están tratando de comunicarse de manera segura. Imagina que deseas enviar un mensaje importante a una persona especial o un amigo, pero aparece un intruso que se interpone en el camino y lee o incluso cambia el mensaje antes de que llegue al destinatario.

Otro ejemplo más acorde, supongamos que estás usando una red Wi-Fi pública en un café para enviar tu contraseña a un sitio web seguro. Un atacante con conocimientos técnicos podría usar software especial para interceptar esa comunicación. Cuando los individuos se conectan a él y acceden a sitios como banca online o e-mail, el atacante podría ver tu contraseña y hasta podría modificarla o bloquearte el acceso al sitio después. Es por eso que es importante usar conexiones seguras y proteger tus datos cuando se navega por internet.

e. Ataques de denegación de servicio (DoS) y DDoS, ataques distribuidos de denegación de servicio

Los ataques de denegación de servicio (DoS) y los ataques distribuidos de denegación de servicio (DDoS) son intentos maliciosos de **interrumpir el funcionamiento** normal de un servicio, sitio web o red, haciéndolos inaccesibles para los usuarios legítimos.

- **Ataques de Denegación de Servicio (DoS)**

Un ataque DoS se realiza generalmente **desde un solo equipo**. El atacante envía una gran cantidad de solicitudes al servidor objetivo, sobrecargándolo y provocando que no pueda manejar las solicitudes legítimas.

Para entenderlo mejor, imagina que hay una tienda pequeña que solo puede atender a 10 personas a la vez. Si de repente 100 personas intentan entrar al mismo tiempo, la tienda se llena y las personas que realmente quieren comprar algo no pueden entrar. Esto es lo que pasa en un ataque DoS: el servidor se satura con tantas solicitudes que no puede atender a los usuarios normales.

- **Ataques Distribuidos de Denegación de Servicio (DDoS)**

Un ataque DDoS es similar a un ataque DoS, pero mucho más potente y difícil de detener porque **proviene de múltiples computadoras** o dispositivos, generalmente controlados por el atacante mediante una red de bots (botnet).

Usando el mismo ejemplo de la tienda, imagina que en lugar de 100 personas, hay 1000 personas distribuidas en diferentes lugares (todos dirigidos por un organizador malicioso) que intentan entrar a la tienda al mismo tiempo. Como hay muchas más personas desde diferentes lugares intentando entrar a la vez, la tienda no solo se llena, sino que también se hace mucho más difícil de manejar y controlar.

Ambos tipos de ataques tienen como objetivo interrumpir el servicio para que los usuarios que de verdad están interesados en nuestro contenido no puedan acceder a nuestros sitios.

f. Cuentas de usuario comprometidas

Una cuenta de usuario comprometida es una cuenta que ha sido accedida sin permiso por alguien más, generalmente a través de métodos engañosos o adivinando contraseñas. Esto puede llevar al **robo de identidad**, acceso a información sensible, y otros problemas serios. Usar contraseñas fuertes y habilitar la doble autenticación puede ayudar a proteger tus cuentas.

Es importante tomar en cuenta que uno de los objetivos prioritarios de la mayoría de los atacantes consiste en robar el acceso a información que aún no se genera. Por ende, las cuentas de usuario, como las de e-mail y redes sociales, pueden comprometerse de diversas formas. Mediante un ataque de phishing se puede instalar malware en el dispositivo y, así, registrar las pulsaciones del teclado de su dispositivo y capturar contraseñas y otra información sensible.

Un atacante también puede utilizar un sitio web falso y, después de que el usuario introduce su información de acceso, el atacante puede entonces utilizarla para acceder al sitio web real sin alertar al usuario. La autenticación de dos factores ayuda a evitar que una cuenta sea comprometida pues requiere tanto la clave de acceso a la cuenta como el dispositivo para acceder (un teléfono celular, por ejemplo), el cual recibe un código de uso único para iniciar la sesión. Desafortunadamente, incluso la autenticación de dos factores puede verse comprometida si el atacante posee los conocimientos necesarios.

g. Intimidación, acoso y exposición forzada de redes online

La intimidación, el acoso y la exposición forzada en redes online son comportamientos dañinos que pueden tener graves consecuencias para la víctima. Estos comportamientos incluyen **enviar mensajes amenazantes**, acosar a alguien repetidamente, o compartir información privada sin permiso. Por ello es importante proteger tu privacidad, ser consciente de lo que compartes en línea y saber cómo reportar y bloquear a los acosadores.

A continuación, se desglosará cada uno de estos términos para entenderlos mejor:

- **Intimidación Online**

La intimidación online, también conocida como ciberbullying, es cuando una persona o grupo de personas utilizan internet para herir, asustar o molestar a otra persona de manera repetitiva y deliberada.

- **Acoso Online**

El acoso online es similar a la intimidación, pero puede ser más persistente y dirigido. Implica comportamientos repetitivos y no deseados que causan angustia o miedo a la víctima. Algunos de los ejemplos pueden ser:

- Publicar fotos privadas de alguien sin su permiso.

- Compartir información personal, como direcciones o números de teléfono, en foros públicos.

Las amenazas físicas y digitales suponen una grave preocupación pues pueden ser la antesala para ataques contra comunicadores, activistas y defensores de derechos humanos. Según investigaciones del Comité para la Protección de los Periodistas, el 38% de los periodistas asesinados en los últimos 21 años fueron amenazados mediante internet antes de ser victimados. (Henrichsen, J. R., Betz, M., & Lisosky, J. M. 2016)

h. Campañas de desinformación y difamación

Las campañas de desinformación y difamación son esfuerzos deli-berados para difundir **información falsa o dañina** sobre una persona, grupo o tema, con la intención de engañar, confundir o perjudicar.

• Desinformación

La desinformación es la difusión de información falsa o engañosa de manera intencional. Su objetivo es confundir a las personas, crear dudas o influir en sus opiniones y decisiones.

• Difamación

La difamación es la acción de **dañar la reputación** de una persona, grupo u organización mediante la difusión de información falsa o perjudicial. Esto se hace con la intención de hacer que otros piensen negativamente sobre la persona o entidad difamada.

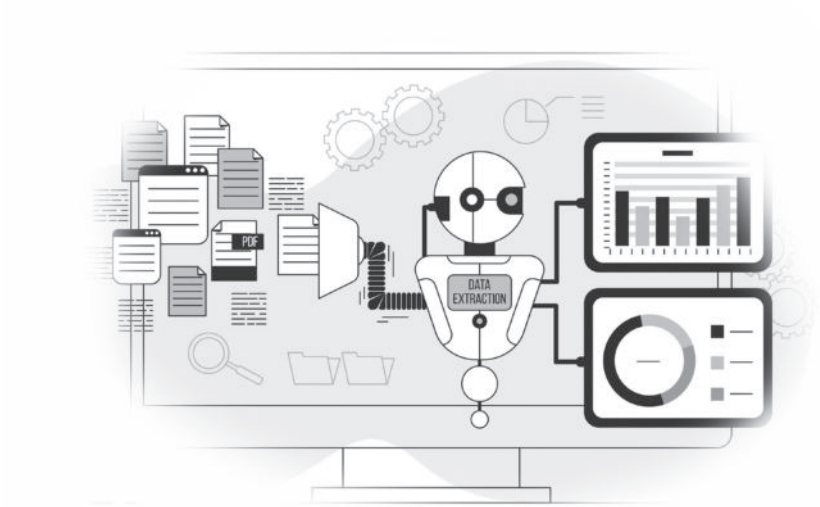
Cómo Funcionan las Campañas de Desinformación y Difamación:

- Creación de Contenido Falso: Los responsables crean noticias, imágenes, videos u otros tipos de contenido que parecen reales pero que son falsos o engañosos.

- Difusión en Redes Sociales: Usan plataformas como Facebook, Twitter, o WhatsApp para compartir este contenido, haciéndolo llegar a un gran número de personas rápidamente.

- Manipulación de Opinión: A través de la repetición y la presentación convincente, logran que la gente crea en esta información falsa y actúe o piense de acuerdo con ella.

- Uso de Bots y Cuentas Falsas: A veces utilizan bots (programas automatizados) o cuentas falsas para amplificar el alcance de la desinformación y hacer que parezca que muchas personas están de acuerdo o compartiendo la misma opinión.



i. Almacenamiento y extracción de datos

El almacenamiento y la extracción de datos son procesos fundamentales en el manejo de información.

• Almacenamiento de Datos

El almacenamiento de datos es el proceso de **guardar información** en algún tipo de medio (como discos duros, servidores, o la nube) para que pueda ser utilizada más tarde. Los datos pueden ser cualquier cosa, desde documentos y fotos hasta registros de transacciones y datos de usuarios.

Un ejemplo es cuando tomas una foto con tu teléfono, esta se guarda en la memoria del dispositivo. Si usas un servicio como Google Fotos, la foto también se guarda en la nube, que es un servidor remoto que almacena tus datos para que puedas acceder a ellos desde cualquier lugar.

El almacenamiento de datos se ha vuelto cada vez más barato y más eficiente, permitiendo que se recopilen y almacenen –incluyendo el contenido de e-mails, textos y otras comunicaciones– durante periodos más largos. Esto facilita la extracción de datos, entendido como búsqueda mediante información computarizada para encontrar patrones o tendencias útiles. En este sentido, existe un importante mercado para analizar datos masivos y muchas de las empresas que suministran datos de consumidores a sitios como Facebook son las mismas que suministran información a agencias de inteligencia y de seguridad, sin ningún tipo de control o contrapeso.

• Extracción de Datos

La extracción de datos es el proceso de recuperar datos específicos de un lugar donde están almacenados. Esto puede implicar buscar datos en bases de datos, archivos, o cualquier otro sistema de almacenamiento para usarlos o analizarlos.

• ¿Por qué es importante?

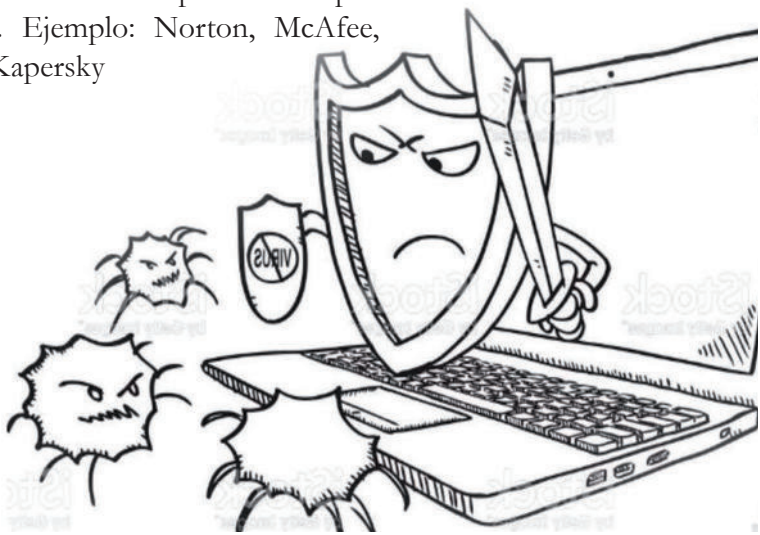
- Accesibilidad: Permite que la información esté disponible cuando la necesites.
- Organización: Ayuda a mantener los datos organizados y fáciles de encontrar.
- Seguridad: Los datos almacenados correctamente pueden protegerse contra pérdidas o accesos no autorizados.

3. Herramientas

Las herramientas de seguridad digital son programas y servicios diseñados para proteger dispositivos, redes, y datos contra amenazas cibernéticas. Estas herramientas ayudan a prevenir, detectar, y responder a incidentes de seguridad, asegurando la integridad, confidencialidad y disponibilidad de la información. (Córdova, Ibañez, Finlay. Mayo, 2021). A continuación, se presenta una descripción de algunas de las principales categorías de herramientas de seguridad digital:

a. Antivirus y Antimalware

Detectan y eliminan software malicioso que puede robar información, dañar sistemas o comprometer la privacidad. Ejemplo: Norton, McAfee, Avast, Kapersky



b. Firewalls

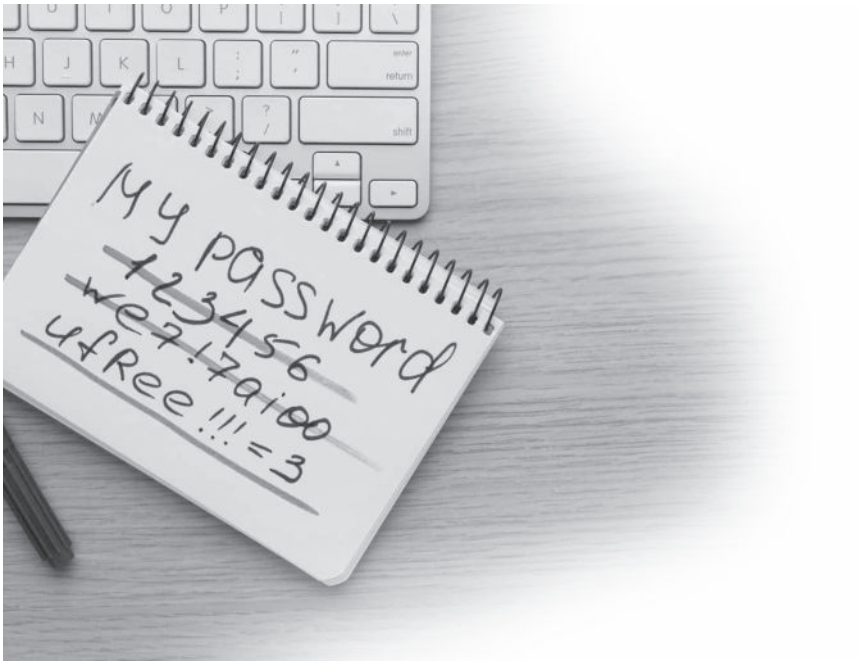
Bloquean accesos no autorizados y previenen ataques de red como el hacking y el phishing.

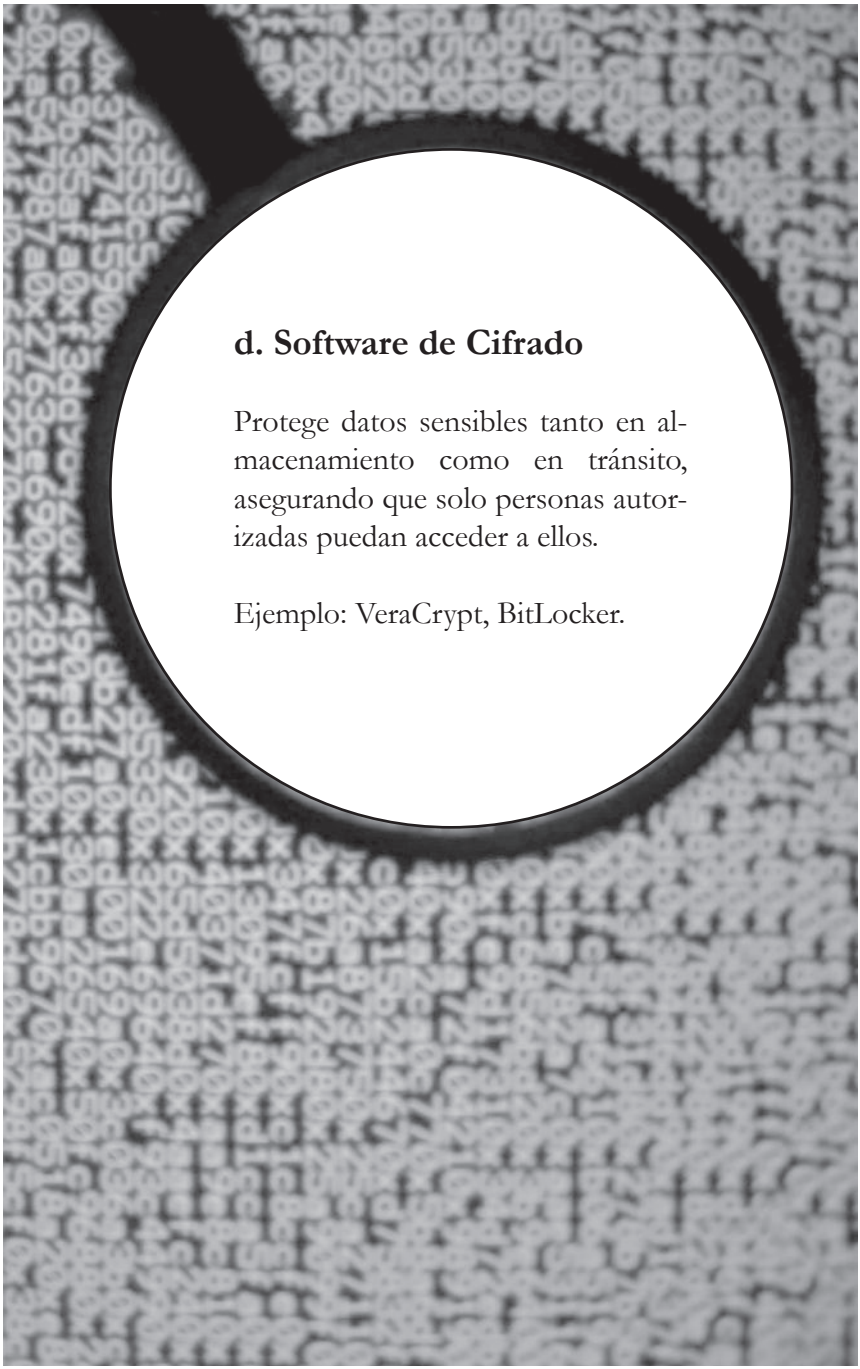
Ejemplo: ZoneAlarm, Windows Defender Firewall.

c. Gestores de contraseñas

Facilitan la creación y almacenamiento de contraseñas fuertes y únicas para cada cuenta, reduciendo el riesgo de robo de credenciales.

Ejemplo: Keepass





d. Software de Cifrado

Protege datos sensibles tanto en almacenamiento como en tránsito, asegurando que solo personas autorizadas puedan acceder a ellos.

Ejemplo: VeraCrypt, BitLocker.

e. Herramientas de Diagnóstico y Evaluación de Vulnerabilidades

Función: Analizar sistemas y redes en busca de vulnerabilidades que puedan ser explotadas.

Ejemplo: Nessus, OpenVAS.

f. Redes Privadas Virtuales (VPN)

Cifran el tráfico de internet, protegiendo la información personal y las actividades en línea de ser monitoreadas o interceptadas.

Ejemplo: NordVPN, ExpressVPN. RiseUp VPN

El uso de herramientas de seguridad digital ofrece una amplia gama de bene-ficios que ayudan a proteger tanto a individuos como a organizaciones de diversas amenazas cibernéticas.

4. Buenas prácticas

Una vez revisadas las herramientas disponibles, es crucial considerar cómo podemos emplearlas para proteger nuestros dispositivos. Las buenas prácticas en seguridad digital consisten en hábitos y estrategias que garantizan la protección de nuestra información personal y profesional en el entorno digital. Estas prácticas están diseñadas para prevenir accesos no autorizados, proteger nuestros datos contra pérdidas y mitigar el riesgo de amenazas cibernéticas como malware, phishing y otros ataques. A continuación, se detallan algunas de las prácticas que usamos como organización.

a. Contraseñas

Las contraseñas son las puertas de entrada a nuestro correo electrónico, perfil en redes sociales y demás servicios online que utilizamos en nuestro día a día en Internet.

Recomendaciones:

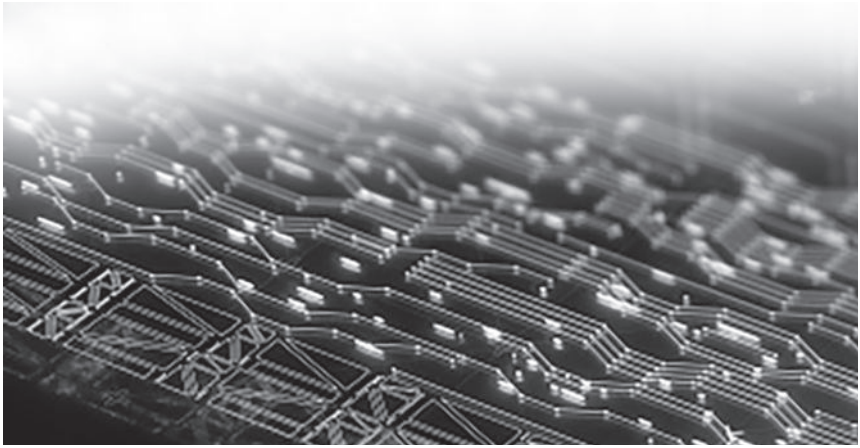
- **Usar siempre contraseñas largas** (mínimo de ocho caracteres) en las que se combinen letras, números y caracteres especiales (-·$%/&), y cámbialas cada tres o seis meses.

- **Nunca repitas las mismas** claves para diferentes perfiles, cuentas de correo, etc.

- No utilices nombres, ni de personajes de ficción (Tampoco utilices otros datos como matrículas, teléfonos, cédula, etc.)

- Crea contraseñas únicas para cada sitio: Hay herramientas que te ayudarán a gestionar esta información. (gestor de contraseñas, Keepass)

- No revele tus contraseñas a nadie



b. Las redes WIFI públicas

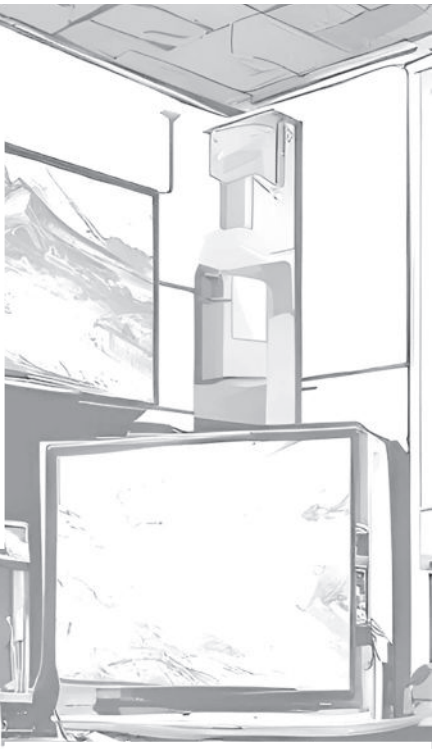
Las redes WiFi públicas son redes inalámbricas disponibles para el uso general en lugares públicos como cafeterías, aeropuertos, hoteles, centros comerciales, y otros espacios similares. Estas redes permiten a los usuarios conectarse a internet de forma inalámbrica utilizando dispositivos como teléfonos inteligentes, tabletas, computadoras portátiles, y otros dispositivos compatibles con WiFi.

Recomendación:

- Si vas a utilizar una red WIFI pública es mejor evitar acceder a servicios (cuentas bancarias, redes sociales, correo electrónico, etc) que requieran introducir una contraseña. **Evita revelar cualquier tipo de dato personal** porque puede ser recopilado por otras personas"

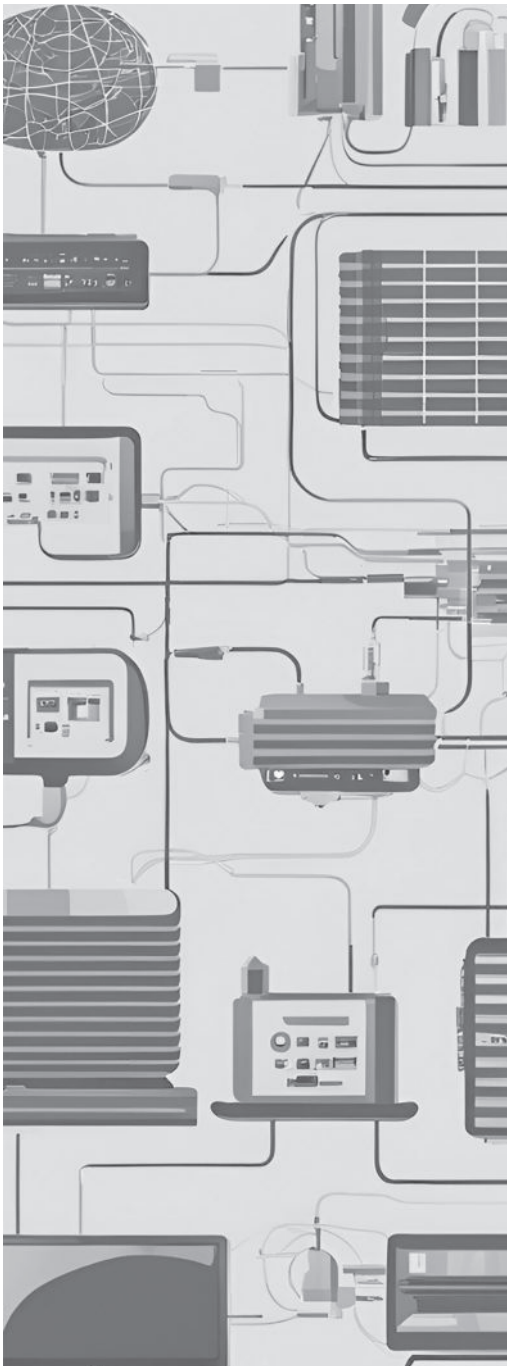
c. Router

Un router es un dispositivo de red que se utiliza para dirigir el tráfico de datos entre redes informáticas. es esencial para la conectividad tanto domésticas como empresariales, proporcionando la infraestructura necesaria para la comunicación efectiva entre dispositivos y el acceso a Internet.



Recomendación:

Configura la seguridad de tu router de manera adecuada. Al igual que con las contraseñas, es crucial cambiar regularmente los datos de acceso a tu router para evitar accesos no autorizados. Hay numerosos vídeos en YouTube que explican cómo cambiar el nombre de usuario y la contraseña del router según el proveedor de servicio de internet que utilices.



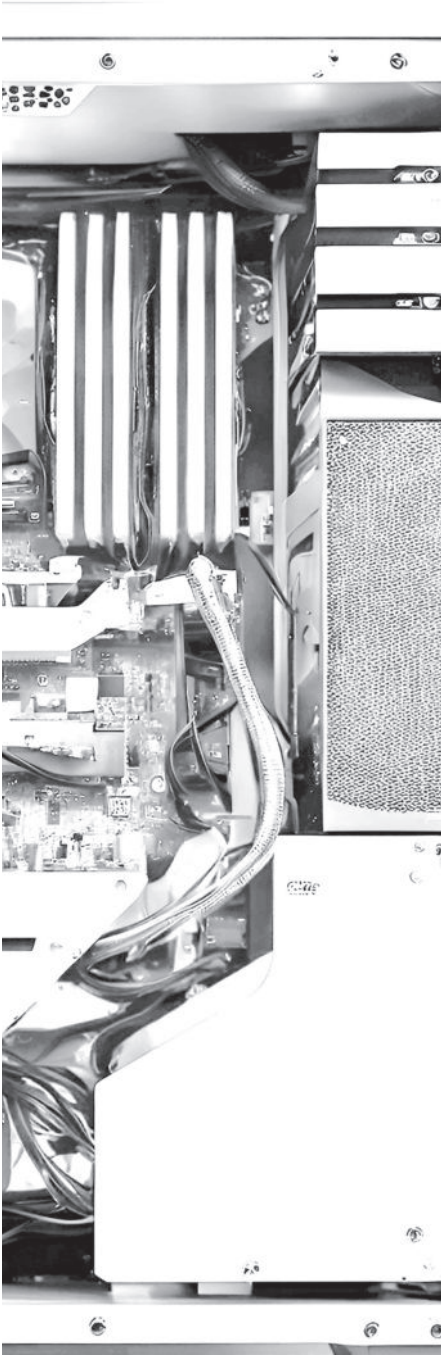
d. PC o Laptop

Una PC o laptop es un dispositivo informático diseñado para ser utilizado por una persona de forma individual. Estos dispositivos son capaces de realizar diversas tareas computacionales, como procesamiento de datos, navegación por internet, creación y edición de documentos, reproducción multimedia, etc.

Recomendaciones:

Mantén el **Sistema operativo** de tu computadora o laptop **actualizado** Cualquier experto en seguridad informática te confirmará que es una medida indispensable para evitar amenazas en Internet. Si tu software no está actualizado estás dejando la puerta abierta al malware que se actualiza y renueva cada día para infectar tu equipo.

Para garantizar una navegación segura en Internet y evitar las amenazas que afectan a tu seguridad informática es indispensable que tengas un **programa antivirus y que esté siempre actualizado** AVG Antivirus, Kapersky son buenas opciones.



Actualizar programas: se recomienda actualizar con los últimos parches de seguridad no solo el sistema operativo, sino también el software o programas instalados en el sistema para evitar la propagación de amenazas.

Al momento de navegar **utiliza https:// y no http://**. En muchas ocasiones alguien podría estar "escuchando" la información que se transmite desde nuestro ordenador, por ejemplo, el tráfico Wifi. Hay muchas aplicaciones y foros en Internet que permiten que un atacante, obtenga nuestras contraseñas. La comunicación https:// viaja encriptada y es más difícil de descifrar y mucho más segura para las redes sociales.

Se precavido cuando utilices una computadora compartida cuando utilices un ordenador que no sea tuyo, ya sea en tu trabajo o en un sitio de internet, **asegúrate de cerrar la sesión** cuando termines de usarlo, no permitas que el navegador recuerde las contraseñas y limitar brindar información personal.

Al Igual que en los dispositivos móviles, se debe cuidar las conexiones entrantes activar el bluetooth y la wifi sólo cuando sea necesario, de forma que no se conviertan en puertas abiertas a posibles intrusos.

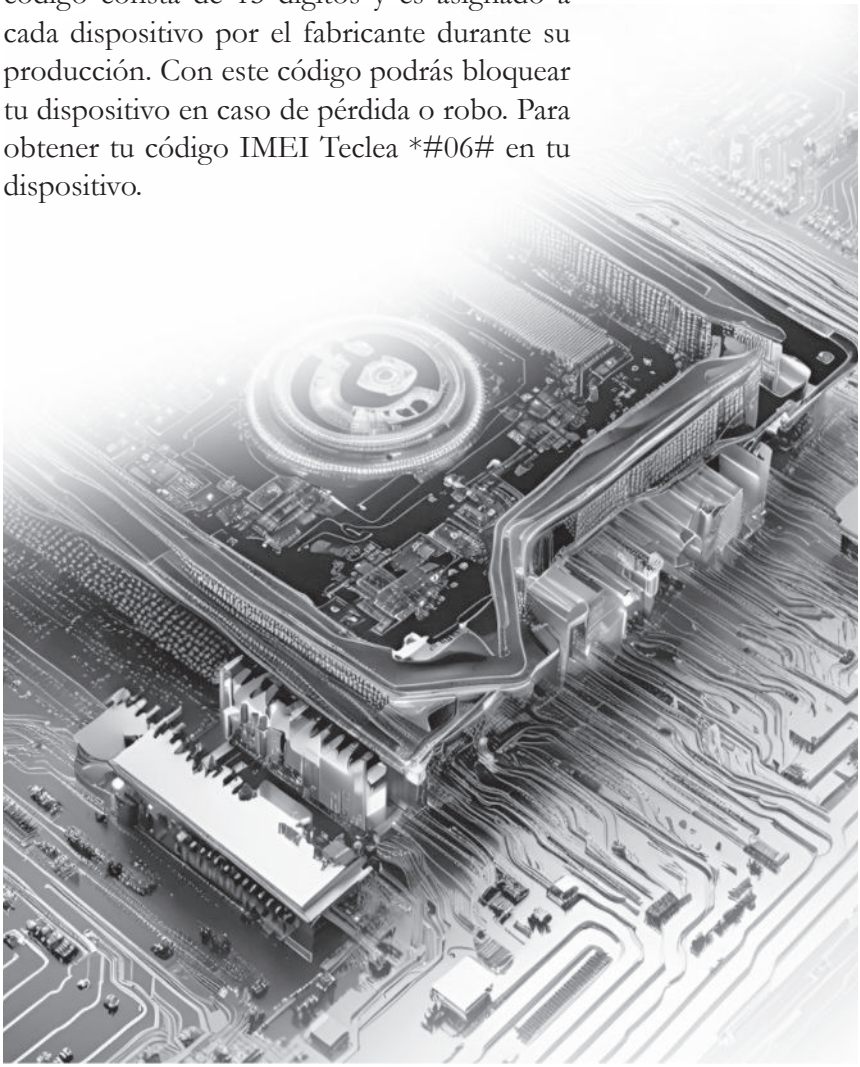
Mantener en correcto funcionamiento las memorias extraíbles: si se comparten tarjetas, memorias USB o dispositivos similares para compartir archivos entre portátiles, tabletas, cámaras de foto y vídeo, etc. recuerda que es necesario analizarlas siempre con un antivirus para asegurarse de que no contienen ninguna amenaza que pudiera distribuirse a los diferentes periféricos.

e. Dispositivo Móvil

Un dispositivo móvil, también conocido como teléfono inteligente, es un dispositivo móvil que combina las funciones de un teléfono celular tradicional con capacidades avanzadas de computación y conectividad. Estos dispositivos permiten a los usuarios realizar una amplia gama de actividades más allá de simplemente hacer llamadas telefónicas. Algunas de sus características distintivas incluyen:

Descarga siempre aplicaciones de las tiendas oficiales (Google Play y App Store) o de aquellas en las que esté acreditada la seguridad en las descargas.

Código IMEI El código IMEI (International Mobile Equipment Identity) es un número único de identificación utilizado para identificar de manera exclusiva a un dispositivo móvil, como teléfonos celulares y smartphones. Este código consta de 15 dígitos y es asignado a cada dispositivo por el fabricante durante su producción. Con este código podrás bloquear tu dispositivo en caso de pérdida o robo. Para obtener tu código IMEI Teclea *#06# en tu dispositivo.



Servicios de mensajería: Todos utilizamos al menos uno. Así como lo hacemos con las redes sociales, es importante tomarse un momento para configurar las opciones de privacidad en WhatsApp o Telegram. De esta manera, podemos revisar qué información estamos compartiendo y qué elementos, como vídeos o fotografías, se descargan directamente en nuestro móvil. Antes de abrir un enlace recibido a través de WhatsApp o Telegram, asegúrate de su fiabilidad.

Antivirus: Es fundamental tenerlo instalado en nuestro dispositivo y configurado para escanear todas las aplicaciones que descarguemos, asegurando así la protección contra posibles amenazas en nuestro dispositivo móvil.

Copia de seguridad: Del mismo modo que en tu ordenador, es importante hacer copias de seguridad periódicas de tus contactos y documentos importantes. Esto te garantiza tener acceso a ellos en caso de problemas con el móvil o amenazas de seguridad.

5. Herramientas de seguridad digital de otras organizaciones

Para culminar este manual, hemos recopilado dos herramientas útiles desarrolladas por varias organizaciones a nivel internacional que trabajan en seguridad digital enfocada para periodistas y defensores de los derechos humanos.

a. Kit de Primero Auxilios Digitales

La Red de Respuesta Rápida es una red internacional de personas que ofrecen respuesta rápida y organizaciones referencia en seguridad digital entre las cuales se encuentran Access Now, Amnesty Tech, Center for Digital Resilience, CIRCL, EFF, Fembloc, Freedom House, Front Line Defenders, Global Voices, Greenhost, Hivos y Digital Defenders Partnership, Internews, La Labomedia, Open Technology Fund, Virtualroad, así como otras personas colaboradoras expertas que trabajan en este campo han desarrollado el Kit de Primeros Auxilios Digitales.

El cual es un recurso gratuito para ayudar a quienes brindan respuesta rápida, formadores en seguridad digital y ac-

tivistas con intereses técnicos a protegerse mejor a sí mismos y a sus comunidades contra los tipos más comunes de emergencias digitales. También puede ser usado por activistas, defensores de derechos humanos, blogueros, periodistas o activistas de medios que quieran aprender más sobre cómo protegerse a sí mismos y ayudar a otras personas. Si tu o alguien a quien estás ayudando está sufriendo una emergencia digital, el Kit de Primeros Auxilios Digitales te ayudará a diagnosticar los problemas que estás experimentando y te referirá a proveedores de soporte adecuados para obtener ayuda más especializada en caso de ser necesario.

https://digitalfirstaid.org/es/

b. Shira

La iniciativa de Front Line Defenders es Shira que ayuda a los usuarios a desarrollar las habilidades necesarias para identificar y vencer los ataques de phishing en aplicaciones de mensajería y correo electrónico. Su metodología es simple y basta con responder un cuestio-nario. La herramienta cuenta con su traducción al castellano.

https://shira.app/

Bibliografía

Manuales

- Arango Gomez, O. D. (2023). El ABC de la seguridad informática: guía práctica para entender la seguridad digital. https://www.autoreseditores. com/libro/22997/oscar-dario-arango-gomez/el-abc-de-la-seguridad-informatica-guia-practica-para-entender. Html.

- Aycardi, G. A. R., & Joseph, P. (2017). Recomendaciones para estimular la Seguridad Digital Ciudadana. Investigación y desarrollo en TIC, 8(2), 29-40

- Córdova Páez Anais, Ibañez Edison, Finlay Jonathan. (Mayo, 2021). Defensa digital para organizaciones sociales. La libre

- Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2016). Cómo desarrollar la seguridad digital para el periodismo: una encuesta sobre temas escogidos.

- Reigada, A. T. (2018). Del principio de seguridad de los datos al derecho a la seguridad digital. Economía industrial, 410, 127-151.

Páginas Web

- Shelter city. Recursos para defensores de Derechos Humanos. Recuperado de: https://sheltercity.org/resources/

- Red de Respuesta Rápida y CiviCERT. Digital First Aid Kit. Re-

uperado de: https://digitalfirstaid.org/es/about/

- Horizontal, Front Line Defender. Shira Recuperado de: https://shira.app/

Video foro

- Access Now. (17 de junio del 20221). RightsCON Recuperado de: https://www.youtube.com/watch?v=t9Jwa_E62RQ&list=PLprTandRM962kq7fcetWh8Uvp0bB0tM8C

ISBN: 978-9978-980-66-8

El Presente manual fue realizado por INREDH,
con el apoyo de la Fundación Nacional
por la Democracia, NED.

NED
NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD