FUNDA REDES

MANUAL

SEGURIDAD DIGITAL Y VERIFICACIÓN DE INFORMACIÓN

www.fundaredes.org



¿QUÉ ES SEGURIDAD DIGITAL?

En la era digital, los equipos electrónicos y la información manejada por los Activistas y Defensores de Derechos Humanos también están en riesgo.

La seguridad digital consiste en capas de protección de los equipos electrónicos y la información digitalizada; está compuesta por un conjunto de herramientas, hábitos y métodos.



¿PARA QUÉ SIRVE LA SEGURIDAD DIGITAL?

Para prevenir el acceso no autorizado, la manipulación o la destrucción de información confidencial y sensible. Las medidas de seguridad digital permiten garantizar la integridad, disponibilidad y confidencialidad de los datos, así como la protección de la privacidad de los usuarios.

Hablar de seguridad digital es buscar la forma de mantener actualizada la protección, información y los datos en el entorno digital.

A Permite cambios en los comportamientos personales, nuestra responsabilidad fortalecerá la tecnología, a su vez ayuda a prevenir errores, tener conciencia y reforzar conductas para su uso adecuado.

B Mejora las formas de cifrar envíos y recepción de mensajes individuales.

C Reduce la vulneración de computadoras y teléfonos a ataques externos.

D Evita el bloqueo de sitios que hacen seguimiento y cifrado de tráfico de internet, impide el seguimiento en línea, robo de cuenta, censura, mapeo en RRSS, etc.

CAMPOS QUE CUBRE LA SEGURIDAD DIGITAL

A  **Protección de equipos electrónicos**

B  **Navegación de forma segura**

C  **Protección de comunicaciones y archivos seguros**

¿CÓMO PROTEGER LOS EQUIPOS ELECTRÓNICOS?

Mantener un equipo seguro comienza desde la forma o las herramientas que utilices para resguardar la información. **Existen algunos métodos que te ayudarán a mantener tu equipo seguro:**

A **SISTEMA OPERATIVO ACTUALIZADO:** Si el equipo pide actualización, se debe realizar para evitar ser atacado por algún software malicioso. Se recomienda habilitar la opción de actualización automática. Si el software no es original, se corre el riesgo de perder la información.

HERRAMIENTA RECOMENDADA: COMO PAQUETE DE SOFTWARE DE OFICINA LIBRE, GRATUITO Y DE CÓDIGO ABIERTO:(LIBRE OFFICE).



B **ANTIVIRUS- ANTISPYWARE:** Un antivirus es un programa diseñado para detectar, prevenir y eliminar virus informáticos. Estos virus son programas maliciosos que pueden dañar archivos, robar información o incluso tomar el control de tu equipo. Un antispyware es una herramienta que detecta y elimina programas espía (spyware). El spyware es un software que se instala en tu equipo sin tu consentimiento y recopila información sobre tus hábitos de navegación, contraseñas y otros datos personales.

HERRAMIENTAS RECOMENDADAS:

Avira free antivirus

Avast

Malwarebytes

Spybot

VirusTotal

Es una aplicación que se encarga de escanear documentos y URLs, y detectar virus o amenazas.

C **CONTRASEÑAS SEGURAS:** Debes tener contraseñas seguras en todas aquellos equipos y plataformas a los cuales puedas acceder mediante contraseña.

RECOMENDACIONES:

- **No uses información personal.**
- **Usa diferentes contraseñas para diferentes servicios y equipos.**
- **Cambiar las contraseñas con regularidad puede ser contraproducente,** es recomendable crear una fuerte que no necesitará cambios.
- El uso de contraseñas largas y datos menos predecibles crea mayor protección. **Incluye caracteres alfanuméricos, mayúsculas, minúsculas y caracteres especiales. Por ejemplo: MANUALseguridadD1g1!@!**
- **No la apuntes en físico; usa un gestor de contraseñas.**

HERRAMIENTAS RECOMENDADAS:

La aplicación **KASPERSKY** te permite detectar el nivel de seguridad de las contraseñas en aplicaciones y redes sociales. Esta opción te ayuda a saber si realmente cuentas con contraseñas fuertes.

Los gestores de contraseñas permiten a cualquier usuario, de acuerdo a la plataforma o aplicación que se vaya a utilizar, almacenar y cifrar cada una de las contraseñas, y así acceder a ellas de manera rápida y segura.



LastPass



KeePassXC
Para Windows, Mac y Linus



Bitwarden



Strongbox

Es recomendable tener un correo solo para el gestor de contraseñas.

D **VERIFICACIÓN DE 2 PASOS:** Consiste en una doble verificación de tu identidad para poder acceder a un equipo o una plataforma. Además de la contraseña, el equipo o plataforma te pedirá un código u otra forma para verificar tu identidad.

- Puedes usarlo en equipos electrónicos y plataformas digitales.

- **Recomendamos que actives la verificación de dos pasos especialmente en tus redes sociales, como Facebook, Twitter e Instagram.**

HERRAMIENTAS RECOMENDADAS:



Authenticator google



Aegis authenticator

En la actualidad, además de redes sociales donde compartimos información colectivamente, **existen aplicaciones enfocadas en la mensajería instantánea, como Whatsapp, Telegram y Signal.**

Estas aplicaciones, por su parte, cuentan con su propio método de verificación de 2 pasos. **Por ejemplo, Whatsapp te pedirá un pin de 6 dígitos (que debes aprender), además de un código que te llegará por mensaje de texto o llamada telefónica.**

Activando la verificación de dos pasos en las aplicaciones de mensajería instantánea (Whatsapp, Telegram, Signal) incrementarás tu seguridad y podrás evitar que suplanten tu identidad.

¿CÓMO NAVEGAR DE FORMA SEGURA?

La navegación segura es un conjunto de prácticas y herramientas diseñadas para proteger a los usuarios de internet de amenazas como el phishing, malware y virus. **Al navegar de forma segura, reduces el riesgo de que tus datos personales sean robados o que tu dispositivo se infecte con software malicioso.**

RECOMENDACIONES:

- Procura navegar haciendo uso del protocolo HTTPS. **El HTTPS es la versión segura del protocolo HTTP, utilizado para enviar datos entre un navegador web y un sitio web.**
- **Para saber si un sitio web es HTTPS, busca lo siguiente:**
  - **Candado en la barra de direcciones:** la mayoría de los navegadores muestran un pequeño candado a la izquierda de la URL.

- **“https://” al inicio de la URL.**
- **Mensaje de seguridad:** al hacer clic en el candado, puede aparecer un mensaje que confirma que la conexión es segura y te proporciona información sobre el certificado de seguridad del sitio.

- **Evita redes Wi-Fi públicas no seguras.**
- **Sé cauteloso con los enlaces:** no hagas clic en enlaces sospechosos, especialmente, si provienen de remitentes desconocidos.

HERRAMIENTAS RECOMENDADAS:



Chromium es un proyecto de navegador de código abierto.

uBlock origin es una extensión para los navegadores que minimiza el almacenamiento de datos, bloquea uso de procesador, memoria y publicidades molestas.

https everywhere permite ver si estás navegando de forma segura y cifrada

Privacy Badger ayuda a bloquear rastreos, si se abre alguna publicidad los evita.



Cookie AutoDelete controla las cookies, borra automáticamente las no utilizadas de las pestañas cerradas



NoScript para bloquear el Java y Javascript y otros complementos y contenidos de scripts

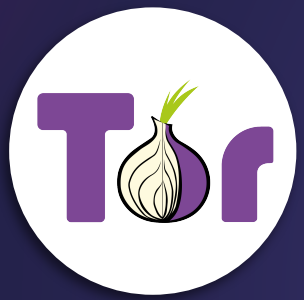
A **VPN:** Una VPN (Red Privada Virtual) es una tecnología que crea una conexión segura y encriptada entre tu dispositivo y un servidor remoto. Esto permite acceder a internet de forma privada y anónima, **ocultando tu dirección IP real y protegiéndote de posibles amenazas en línea.**

Cifrar la información cuando navegas en internet es parte fundamental para proteger lo que investigas o buscas a través del navegador.

Por su parte, una VPN, ayuda a protegerte del rastreo, la vigilancia y la censura, además que encripta y envía todos los datos de internet desde su dirección IP a través de otra.



Proton VPN



Navegador Tor Project



Open VPN



Psiphon VPN



Hideme VPN



Hoxx VPN



Speedify



TunnelBear



Riseup vpn



Your Freedom

¿CÓMO PROTEGER LAS COMUNICACIONES Y ASEGURAR LOS ARCHIVOS?

Una comunicación es segura cuando el riesgo de ser interceptada es mínimo. **Es decir, puedes estar seguro que tú y la otra persona con la que te quieres comunicar, son las únicas personas que conocen el contenido del mensaje transmitido.**

- Usa canales de comunicación con cifrado punto a punto (2P2). **Evita los mensajes de texto y llamadas telefónicas convencionales.**
- **Realiza limpieza constante de las conversaciones, fotos y vídeos en equipos.**
- Evita enviar informaciones de dudosa procedencia,en especial que te **genera algún sentimiento (Rabia, tristeza, alegría). Verifica la información antes de compartirla**

A **MENSAJERÍA INSTANTÁNEA:** Comunícate a través de aplicaciones seguras. Opta por aplicaciones de mensajería instantánea que ofrecen cifrado de extremo a extremo.

Las distintas aplicaciones o redes sociales para comunicación y mensajería que hoy en día son conocidas y manejadas por la sociedad en general, **han generado algunos factores que permiten profundizar sobre la protección, desde datos personales en los móviles hasta información que se puede o no almacenar.**

Entre las aplicaciones más usadas **WhatsApp, Telegram, Signal,** entre otras, lo recomendable es seguir los siguientes pasos:

- **Desactivar copia de seguridad, directamente en ajustes de la aplicación.**
- **Desactivar almacenamiento automático de fotos o videos.**

Mantén activada la seguridad o verificación en dos pasos, esta clave permite ir un paso adelante antes que cualquier agente externo pueda ingresar a tu aplicación o red social, la aplicación te la pedirá con cierta frecuencia.

HERRAMIENTAS RECOMENDADAS:



Wire app Es una aplicación de mensajería diseñada con un fuerte enfoque en la privacidad y la colaboración. Permite enviar mensajes, realizar llamadas de voz y video, compartir archivos y mucho más, con un alto nivel de seguridad. Es una aplicación de código cerrado, es decir, el código no está disponible a cualquier usuario.



Delta chat Es una aplicación descentralizada. Es decir, no depende de servidores centrales, lo que la hace más segura. Delta Chat, además, usa tu dirección de correo electrónico, en vez de tu número telefónico.

B **CORREOS SEGUROS Y CIFRADOS:** Un correo electrónico cifrado es un mensaje que ha sido codificado de tal manera que solo el destinatario autorizado puede descifrarlo y leerlo. Esto significa que si alguien intercepta tu correo electrónico en el camino, no podrá entender su contenido. Usar un correo electrónico cifrado aumenta tu privacidad, confidencialidad y seguridad.

HERRAMIENTAS RECOMENDADAS:

Protonmail

Tutanota

B **LLAMADAS CIFRADAS:** Una de las plataformas utilizadas con más frecuencia es Zoom, sin embargo, existen unas de fácil acceso y con seguridad elevada.

HERRAMIENTAS RECOMENDADAS:



Jitsi meet



BigBlueButton

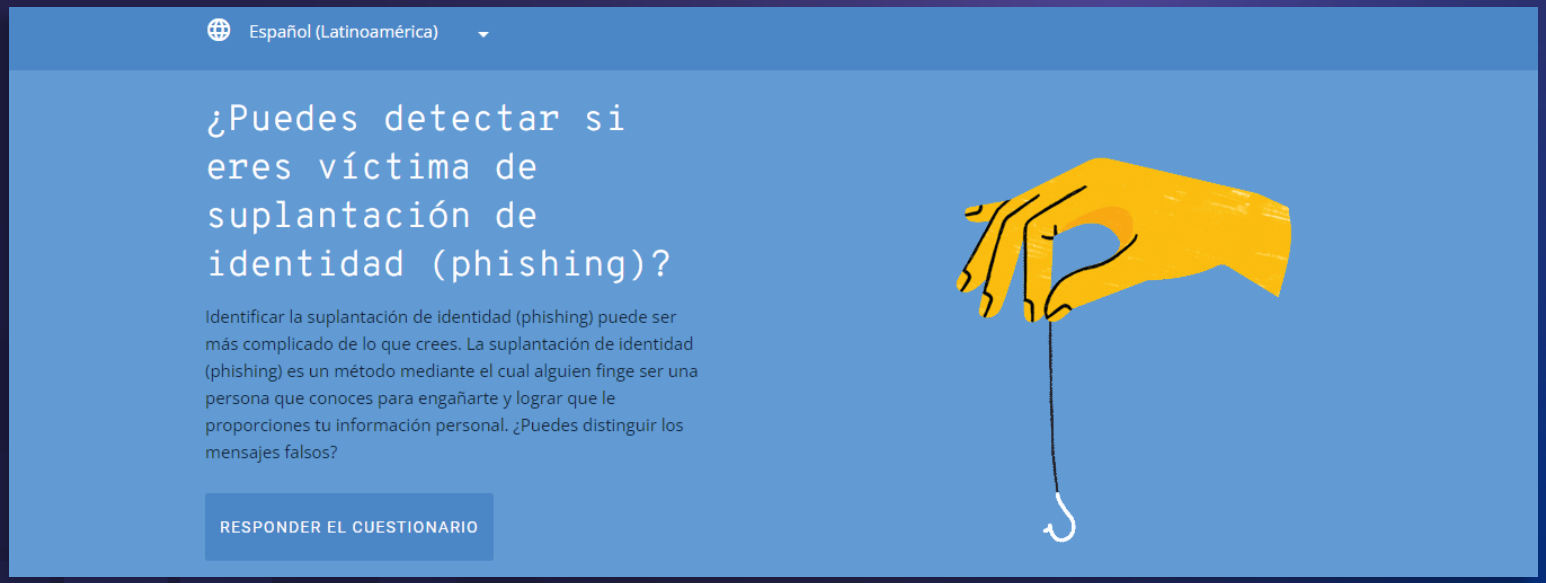
D TRABAJO COLABORATIVO

- **CryptPad.fr** es una suite ofimática colaborativa, completamente encriptada y de código abierto. Esto significa que puedes trabajar en documentos, hojas de cálculo, presentaciones y otros archivos de forma conjunta con otras personas, cumpliendo estándares de seguridad digital.

- **pad.riseup.net** también permite trabajo colaborativo a través de un software libre.

E **PHISHING:** Se refiere al hurto de información a través de correos electrónicos o mensajes en redes sociales que tienen la apariencia de proceder de fuentes de confianza (como bancos, organizaciones sin fines de lucro, amistades, gobiernos.).

Por ejemplo, el phisher (la persona que quiere robar tu información) puede enviarte un correo electrónico desde una cuenta muy similar a la del banco que más usas, o de un ser querido, donde te pide que abras un enlace y con ello poder extraer tu información personal.



HERRAMIENTAS RECOMENDADAS:

Google desarrolló un test que te permite ver si podrías detectar un engaño (Phishing). **El test te plantea información y tú debes descifrar si se trataría de un phishing o de información auténtica.**



https://phishingquiz.withgoogle.com/

F Respaldo de archivos: Un respaldo (backup) es una copia de información para ser usada en caso de que la información original se pierda.

- Es necesario contar con, **al menos, 2 copias de nuestra información en caso de robo, pérdida o daño de equipos.**
- Preferiblemente, **respalda la información en servicios en línea y con verificación de dos pasos.**
- En caso de tener respaldo en físico (discos duros, memorias), **éste debe estar encriptado y en un lugar seguro.**

HERRAMIENTAS RECOMENDADAS:



Sync



Cryptomator



freeFileSync

Si deseas tener una copia de seguridad en la nube, ten en cuenta que solo se almacena online en una red de servidores externos. Es preferible usar una nube cifrada

ENVÍO DE ARCHIVOS PESADOS: Al compartir archivos pesados, opta por plataformas especializadas en transferencias grandes que ofrezcan cifrado de extremo a extremo. Verifica siempre la autenticidad de los enlaces de descarga y asegúrate de que los destinatarios sean de confianza.

HERRAMIENTAS RECOMENDADAS:

share.riseup.net **send.firefox.com** **send.tresorit.com**

I **LIMPIEZA Y BORRADO DE ARCHIVOS:** Al eliminar archivos, asegúrate de utilizar herramientas especializadas que sobrescriban los datos múltiples veces para evitar recuperaciones no autorizadas. **Evita simplemente vaciar la papelera de reciclaje, ya que los datos podrían ser recuperados con software especializado.**

HERRAMIENTAS RECOMENDADAS:

CCleaner herramienta para limpiar el PC. Protege su privacidad y hace que el equipo funcione con mayor rapidez y seguridad. Cuenta versión paga y gratuita.

Eraser creado para borrado más profundo, de código abierto y software libre, ayuda a eliminar archivos permanentemente.



Si eliminaste un archivo por error y deseas recuperarlo, la aplicación Recuva puede ser de utilidad.

VERIFICACIÓN DE INFORMACIÓN

1. ¿Qué es Verificación de Información?

Consiste en analizar críticamente la fuente, el contenido y el contexto de una información **para determinar si es confiable y, por tanto, si se corresponde con la realidad.**

2. ¿Por qué es importante verificar la información?

En la era digital, la información se propaga a ritmos muy rápidos, y es fácil que información falsa se viralice. Verificar la información evita o disminuye la confusión, miedo o polarización que puede ser generado por

información que no es real. Asimismo, verificar la información contribuye en la prevención de la manipulación de la opinión pública, para así mantener un debate público informado y basado en hechos.

3. Conceptos claves

A **INFORMACIÓN FALSA:** Información que no se corresponde con la realidad.

B **INFORMACIÓN ERRÓNEA (MISINFORMACIÓN):** Es información falsa que se comparte sin la intención de engañar. Puede ser compartida por un error, un malentendido o una falta de verificación.

C **DESINFORMACIÓN:** Es información falsa compartida deliberadamente, con el propósito de engañar, manipular o causar daño.

4. ¿Cómo y por qué se propaga la información falsa?

Las informaciones falsas suelen apelar a las emociones, como el miedo, la ira

o la sorpresa. Estas emociones pueden hacer que las personas compartan información sin verificarla. **A eso se suma la confirmación de sesgos: la tendencia a creer en información que se alinee con las opiniones propias preexistentes.**

Las redes sociales son el principal medio para la difusión de información falsa. Una vez que una información falsa comienza a circular, puede generar una reacción en cadena, con cada vez más personas compartiéndola sin verificar su veracidad.

5. ¿Cómo verificar la información?

A **NO TE APRESURES:** Al recibir una información, tómate tu tiempo para preguntarte:

- **¿QUIÉN PUBLICÓ LA INFORMACIÓN?**
- **¿ES UNA FUENTE CONFIABLE?**
- **¿LA FUENTE PUEDE ESTAR SESGADA?**
- **¿LA FUENTE ESTÁ ACTUALIZADA?**

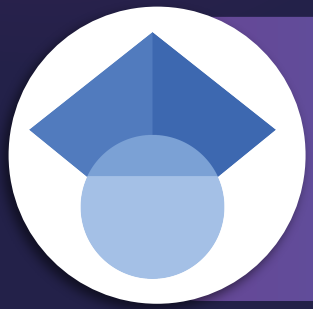
B INVESTIGA Y ANALIZA

- **Averigua** sobre la fuente que publicó la información.
- **Comprueba** las fechas y los contextos.
- **Identifica** posibles inconsistencias o contradicciones.
- **Evalúa el lenguaje utilizado** (emocional, sensacionalista) y busca señales de posible manipulación, como títulos engañosos o citas fuera de contexto.
- **Relaciona la información** con otros eventos o hechos ya verificados.
- **Corrobora la información** con múltiples fuentes, preferiblemente con aquellas que son confiables.

HERRAMIENTAS RECOMENDADAS:



DuckDuckGo es un motor de búsqueda alternativo que cumple con los estándares de privacidad del usuario respecto de la seguridad digital. A través de él, puedes navegar en la web y cotejar la información.



Google Scholar Si la información es de carácter científico, puedes usar motores de búsqueda especializados, como Google Scholar, donde encontrarás contenido académico y científico.



Google Imágenes Permite buscar información a través de imágenes, para así encontrar su origen y posibles manipulaciones.

- **WayBack Machine** permite ver versiones anteriores de páginas web para detectar cambios o eliminaciones de contenido.

- **AFP Fact Check** Existen iniciativas de detección de informaciones falsas, como AFP Fact Check, quienes se encargan de investigar y determinar con evidencia si una información es real o falsa. Te recomendamos buscar iniciativas locales enfocadas en tu región o país.

¡ROMPE LA CADENA!

¡Tú puedes contribuir **a un debate público informado y basado en hechos!**

Recuerda: No te apresures, investiga y analiza.

FUNDA REDES

¡VERIFICA LA INFORMACIÓN Y COMPARTE LA VERDAD!

www.fundaredes.org



MANUAL: SEGURIDAD DIGITAL Y VERIFICACIÓN DE INFORMACIÓN