Privacidad

en

Internet

pd

Introducción

El objetivo de esta guía es poder comprender cómo funcionan algunas de las tecnologías de información y comunicación (TIC) que manejamos a diario, poniendo especial atención en el uso de datos e información que éstas administran y que pueden poner en riesgo la privacidad de las personas si no se las utiliza correctamente.

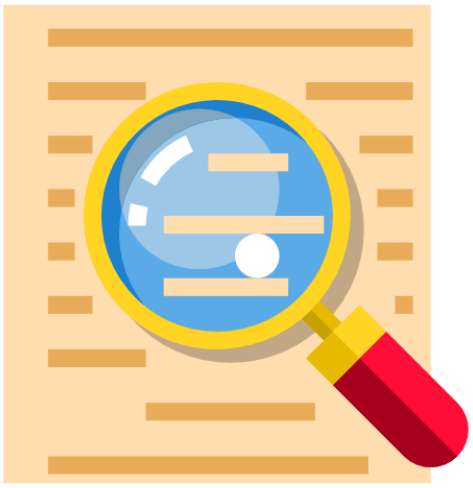
Si bien al día de hoy resulta complejo poder obtener un nivel de privacidad elevado, nuestra labor será comprender qué tan expuestos estamos y cuánto podemos hacer para cambiar esa situación. Cabe destacar que para conseguir un nivel aceptable de privacidad es necesaria una cuota importante de interés por parte de la persona en querer corregir la exposición que hoy en día tiene.

Haremos una recorrida de las configuraciones de seguridad que deberíamos prestar atención siempre que utilicemos un dispositivo móvil, un navegador para surfear la web y al utilizar las redes sociales.

Los temas a trabajar serán:

- Búsqueda de Información Personal
- El arte de recopilar datos de los Usuarios
- La exposición en las Redes Sociales
- Los rastreadores que deambulan en Internet
- Cómo funcionan los Dispositivos Móviles

Búsqueda de **Información Personal**



Búsqueda de **Información Personal en Internet**

Introducción:

Accedemos a Internet todos los días para realizar diferentes actividades tanto en nuestro mundo personal como en el académico. Quizás sin darnos cuenta estamos volcando voluntariamente un sinfín de información personal en las distintas páginas y redes sociales que quedará allí almacenada para siempre si no es que tomamos el debido control. Debemos comprender que todo lo que uno comparte o publica en Internet resulta muy complejo poder eliminarlo de forma definitiva.

Razón por la cual, si queremos tener una huella digital responsable (todos los datos que figuran de mí persona en Internet) y saneada tendremos que ser nosotros quiénes controlemos la existencia de dicha información constantemente para evitar futuros usos incorrectos o que no termine representándonos.

Recomendaciones Previas:

Antes de adentrarnos en la tarea de buscar qué información existe, o está disponible en Internet sobre nosotros, será prudente realizar estos ajustes:

a. Cerrar sesión en todas las cuentas de redes sociales que tengamos abiertas.
b. Cerrar sesión en todas las cuentas de email que tengamos abiertas.
c. Limpiar el historial y toda la información de navegación almacenada en el navegador que utilicemos. **Link**

Actividad:

1. Lo primero que haremos será ingresar en Google y colocar nuestro Nombre y Apellido para ver qué información aparece asociada a esos datos ingresados.

2. Podemos utilizar la búsqueda avanzada de Google para hacer un análisis aún más específico: **Link**

3. También podemos usar otros buscadores como: DuckDuckGo, StartPage, Bing o Yahoo. **Link**

4. Podemos utilizar el buscador de personas PIPL. **Link**

5. Probemos esto: Busquemos una foto donde se vea bien nuestra cara en primer plano y probemos de arrastrarla en el buscador de imágenes de Google a ver qué resultado nos arroja. De esta manera podremos saber si esa foto fue publicada en algún otro sitio y de paso encontrar parecidos nuestros. **Link**

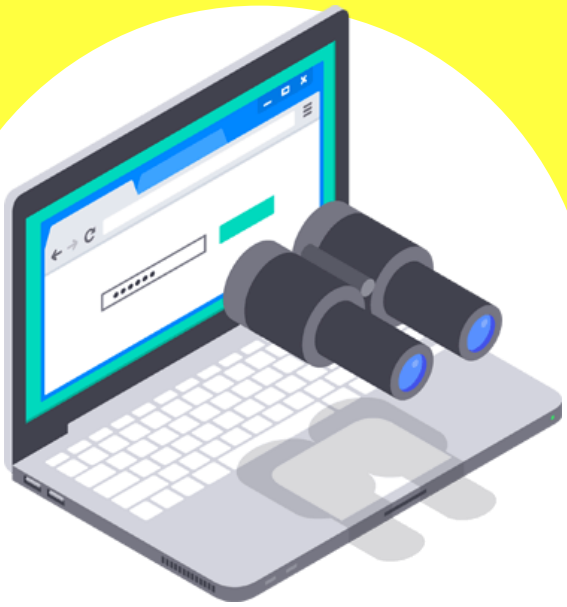
Preguntas:

- ¿Has encontrado información publicada que desconocías que existía?
- ¿Dónde se encuentra almacenada? ¿Es una página web o una red social?
- ¿Es posible eliminar dicha información? ¿Cómo lo harías?
- ¿Es posible contactar al dueño de la página para que remueva esos datos?
- ¿Quién es el dueño de ese contenido, vos o la página o red social que lo tiene almacenado? ¿Por qué?

Consejos:

- De haber encontrado información que no quieras que este visible, intenta contactar al dueño de la página para que la remueva. Según la ley 25.326 de Datos Personales de Argentina, se debe tener el consentimiento de la persona para publicar información personal sobre ella.
- Si lo que encontraste está publicado en alguna de tus redes sociales, deberás revisar y modificar la configuración de privacidad para evitar que esos datos no queden expuestos públicamente a cualquiera en Internet. También prueba removiendo directamente el contenido de la red social para que no esté más disponible.
- Si algún sitio web no quiere remover tú información, podrás hacer la denuncia a la Dirección Nacional de Protección de Datos Personales quienes podrás ayudarte. **Link**
- Es importante que lleves un control regular sobre la información que existe publicada de ti en Internet. No permitas que alguien la utilice con fines incorrectos.

El arte de **recopilar** datos de los usuarios



El arte de **recopilar** datos de los usuarios

Introducción:

La gran mayoría de los servicios que utilizamos a través de Internet recopilan datos sobre nuestra actividad con el objetivo de crear un perfil de usuario, es decir: intereses, gustos, idioma, ubicación, etc. Ese conjunto de información es muy valiosa y en la actualidad se utiliza con fines publicitarios entre otras cosas. Cuanto más se conoce a un usuario, más eficiente se convierte una campaña publicitaria.

Si queremos minimizar o evitar que las empresas proveedoras de servicios obtengan tanta información sobre nosotros y nuestra actividad, debemos controlar cómo tenemos configurado el funcionamiento de las distintas tecnologías que utilizamos a diario. Por cuestiones de difusión y alcance, nos centraremos en Google y Facebook, pero el mismo caso de estudio puede trasladarse a cualquier plataforma.

Actividad:

1. Para conocer qué sabe Google sobre nosotros podremos ingresar a Google MyActivity y verificar todo lo que recopila sobre nuestros movimientos a través de su plataforma. Podremos eliminar toda la información que tiene almacenada, como así también configurar para que deje de almacenarla. **Link**
2. Para conocer qué sabe el Sr. Facebook sobre nosotros podremos descargar un archivo con toda nuestra información e investigar cuánto ha ido almacenando esta red social sobre nuestra actividad. **Link**
3. Del mismo modo, podremos conocer qué sabe Instagram sobre nosotros y descargar un archivo con dicha información. **Link**
4. En caso de utilizar otros servicios o redes sociales en Internet, verificar si podemos obtener qué tanto saben sobre nosotros desde su apartado de seguridad o privacidad. Todos deberían tener esta posibilidad. Si no lo tienen, te recomendamos no usarlos.

Preguntas:

- ¿Considerás correcto que las empresas recopilen tanta información sobre sus usuarios? ¿Por qué?
- ¿Aceptarías pagar por los servicios que utilizás en vez de entregar tanta cantidad de datos a estas empresas por su uso gratuito? ¿Es justo este modelo “gratuito”? ¿Por qué?
- ¿Considerás que las empresas comunican de forma clara y sencilla la información que recopilan sobre sus usuarios? ¿Alguna vez leíste estos contratos de Términos y Condiciones?

Consejos:

- Una buena forma de evitar que una tecnología recopile datos sobre nosotros es cambiar por otra solución o directamente dejar de utilizarla. Como sabemos que probablemente no dejarás de utilizar nada, te ofrecemos un listado con algunas alternativas interesantes. Por ejemplo:
    1. Windows o OS: Linux
    2. Búsquedas con Google: DuckDuckGo o StartPage

3. Gmail: ProtonMail
4. WhatsApp: Telegram / Signal

De esa manera evitaremos tener concentrada en una única empresa muchos servicios como sucede con Google. En el siguiente link podrás encontrar un listado de alternativas disponibles para la gran mayoría de los servicios que utilizas a diario. **Link**

- Si decidís no cambiar de plataforma tecnológica y quedarte donde estás, toma como buena práctica revisar la configuración que tienen tus redes sociales y demás servicios en pos de evitar que sigan obteniendo datos personales sobre tú actividad en Internet.

La exposición en **Redes Sociales**

La exposición en **Redes Sociales**

Introducción:

Sin lugar a duda una de las cosas que más utilizamos en Internet son las Redes Sociales. Fueron construidas y diseñadas desde su esencia para lograr que las personas se comuniquen e intercambien contenido de todo tipo, son muy sencillas de manejar y nuestro principal pasatiempo digital en los días que corren.

No obstante, la configuración de seguridad por defecto que traen deja mucho que desear. Un claro ejemplo de ello es que cada vez que creamos un perfil el mismo se configura de forma pública. Lamentablemente es el usuario quién debe configurar su perfil para que quede en modo privado. Si es que así lo desea...(¿?)

Como dice Dara Boyd... **"Somos públicos por defecto y privados a través del esfuerzo"**

Actividad:

- Ingresar a cada una de las redes sociales que utilicemos, y verificar cómo está configurada la Privacidad. Deberíamos evitar, en la medida de lo posible, configuraciones públicas de nuestros perfiles.
- Adicionalmente sería una buena práctica revisar qué Contactos tenemos en nuestras redes. Por lo general se suele acumular muchas personas que no conocemos. Una buena depuración de contactos evitará que estemos tan expuestos.
- Podemos hacer una revisión de nuestra Biografía o Historial para identificar todas las fotos, videos y comentarios en lxs que estamos etiquetadxs, ya sean nuestras o publicadas por terceros. Aquellxs que consideramos que nos pueden exponer, como podría ser mencionar dónde vivimos, el colegio al cual vamos, etc. deberíamos removerlas para que nadie las vea.

- También podemos realizar una búsqueda intensiva por los perfiles de nuestros principales contactos para identificar si han publicado datos personales nuestros. De encontrar, deberíamos solicitarles que los remuevan, ya que deberían haber solicitado nuestro consentimiento para hacerlo.
- Verificar cómo tenemos configurada la función de Geolocalización dentro de la red social. Algunas de ellas tienen la posibilidad de informar en tiempo real dónde estamos. Lo cual es muy inseguro. Snapchat y WhatsApp son un claro ejemplo.
- En caso de ser usuario de Facebook, podemos instalar el complemento para navegadores (Firefox/Chrome, etc.) llamado DataSelfie, el cual nos mostrará cómo esta red social analiza nuestros movimientos generando un perfil determinado al cual luego puede direccionarle publicidad. Será una forma de comprender el funcionamiento de su algoritmo. **Link**

Preguntas:

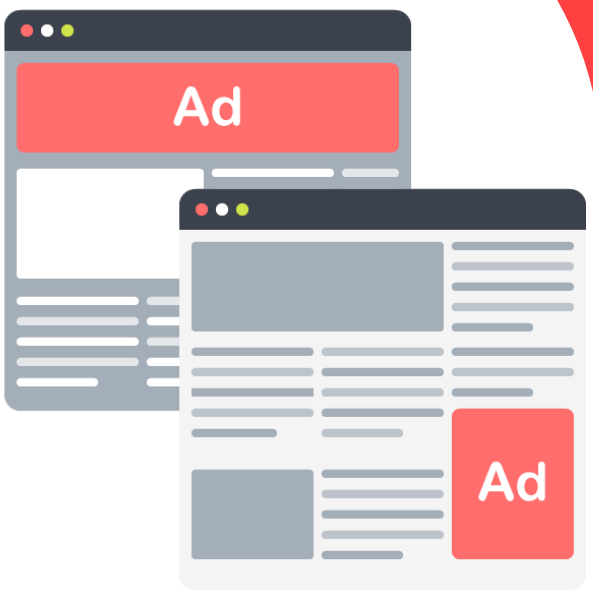
- ¿Cómo encontraste configurada la privacidad de tus distintas redes sociales? ¿Tenías muchas funciones configuradas en modo público?
- ¿Tenías contactos desconocidos en tus redes que podían tener acceso a todo lo que vos publicabas? ¿Decidiste eliminarlos o pensás continuar con ellos?
- ¿Encontraste alguna foto/video o comentario en tú biografía o historial que tenía datos personales tuyos y te comprometían? ¿Decidiste eliminar esa información?
- ¿Cuáles serían los riesgos de tener perfiles públicos en las redes sociales?

Consejos:

- Siempre que comiences a utilizar un servicio en Internet, sea una red social o página web, verifica cómo tiene configurada la privacidad. De esta manera harás un uso seguro desde el comienzo.

- Evita publicar contenido que muestre datos personales tuyos o de personas que conozcas.
- Evita agregar personas desconocidas a tus redes sociales, nunca se sabe quién puede estar detrás de una pantalla.
- Si te interesa, te ofrecemos mirar y participar de un documental interactivo canadiense llamado **“IN LIMBO”,** el cual demostrará cómo las empresas utilizan nuestra información, los permisos que cedemos a los distintos dispositivos y cómo si no tomamos conciencia de la importancia de la privacidad, los únicos que nos perjudicamos en un futuro seremos nosotros. Te recomendamos hacerlo desde una notebook o celular. **Link**

Los Rastreadores de Internet



Los rastreadores que deambulan en Internet

Introducción:

En este apartado vamos a hablar sobre la utilización de una tecnología presente en la gran mayoría de las páginas y servicios que usamos a diario en Internet, los trackers o rastreadores web.

Esta tecnología es la encargada de realizar el análisis y seguimiento de la actividad web de los usuarios en Internet. Los trackers se encuentran presentes en la gran mayoría de páginas web monitoreando nuestra localización, la cantidad de veces que accedemos, a qué le hacemos clic y demás información que pueda resultarles interesante. Seguramente alguna vez habrán estado navegando por sitios de compras buscando algún producto y luego, al estar en alguna red social, vemos que aparecen anuncios relacionados a ese producto que estuvimos buscando. Bueno, eso se debe al trabajo que hacen los rastreadores!

Actividad:

1. Vamos a abrir nuestro navegador preferido e instalar en complemento llamado Lightbeam para Firefox **(link)** o Disconnect en Google Chrome **(link).** Una vez hecho esto, ingresaremos por ejemplo en aliexpress.com y veremos todos los rastreadores que tiene dicha página. Así podremos repetir con la página que deseemos para ver si somos rastreados y por quién. **Link**
2. Si nos interesa podemos utilizar la siguiente página: http://cyslabs.mywebcommunity.org/ Esta nos mostrará información que podría ser recopilada por cualquier página que tenga la tecnología como para hacerlo.
3. Vamos a probar un desarrollo de la organización EFF llamado: Panopticlick para testear nuestro navegador web y comprobar si evita que las páginas rastreen nuestra actividad web. **Link**
4. Ingresaremos en el menú de opciones del navegador, y verificaremos si tenemos asignado algún permiso en alguna página:

- En Firefox: Menú/Opciones/Privacidad y Seguridad/Permisos
- En Chrome: Menú/Configuración/Configuración Avanzada/Configuración de Contenido

Preguntas

- ¿Alguna vez habías pensado que por el simple hecho de navegar estarías siendo monitoreado? ¿Cuál fue la página con mayor cantidad de rastreadores que encontraste?
- ¿Considerás que es correcto que te rastreen mientras navegás sin ser informado por ello? ¿Por qué?
- ¿Cuál fue el resultado del test de tú navegador realizado por la herramienta Panopticlick? ¿Es seguro tú navegador? ¿Evita que te rastreen?
- ¿Tenías otorgados permisos a páginas que hayas visitado? ¿Los has removido?
- ¿Sabías que son las famosas Cookies que aparecen cada vez que ingresamos a un sitio web? Si no sabías aquí podés averiguarlo: **link**

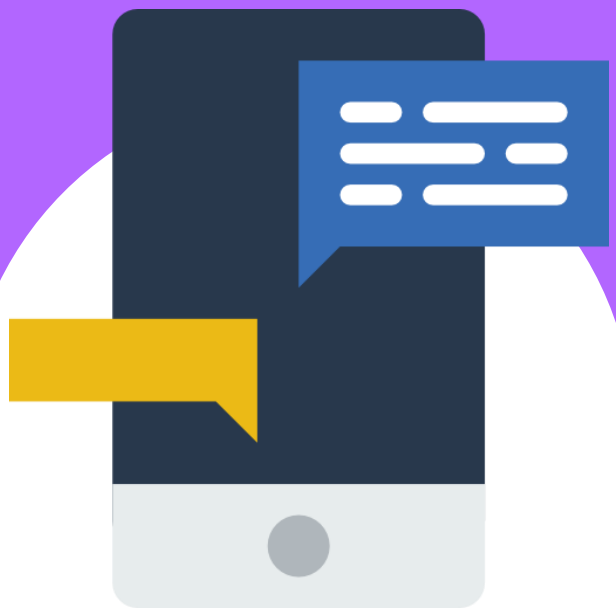
Consejos:

Intentaremos minimizar el efecto de los rastreadores mediante el uso de algunas herramientas de seguridad. Lamentablemente no se puede garantizar que no seremos trackeados de forma absoluta pero sí que nuestra monitorización disminuirá.

- Para controlar y minimizar el rastreo podemos utilizar complementos como Ghostery / Privacy Badger / Disconect.me todos disponibles para la gran mayoría de los navegadores. **link**
- Para evitar la excesiva publicidad que tienen algunas páginas web, instalaremos complementos de bloqueo de anuncios: uBlock o Ad Block Plus funcionan muy bien para evitar esto. **link**
- Una buena práctica a la hora de realizar compras por Internet, es evitar que los sitios web almacenen sus cookies (archivos de seguimiento) en nuestros equipos. Para eso podemos usar la navegación oculta o privada. De esta manera el navegador evitará que se almacene localmente estas “galletas de seguimiento”.

- Si queremos evitar que nuestra dirección IP sea conocida al navegar por las distintas páginas y servicios podemos instalarnos una VPN. Buenas opciones para estas son: ProtonVPN y NordVPN. **link**
- Por último, una buena forma de evitar que nos monitoricen es cambiando nuestro servicios principales, si usamos Google para búsquedas, seguramente seremos rastreados, pero cambiando a otra tecnología como DuckDuckGo, lo evitaremos. **Link**
- Debemos tener presente que nunca deberíamos guardar datos personales en los navegadores (contraseñas, etc.) ya que es muy sencillo obtenerlas. Por tal razón será bueno comprobar si hemos guardado en el navegador alguna password sin darnos cuenta: "Menú/Opciones/Privacidad y Seguridad/ Formularios y contraseñas" en Firefox.
- Por otro lado, debemos revisar qué permisos les hemos dado a las páginas en nuestro navegador sin darnos cuenta: "Menú/Opciones/Privacidad y Seguridad/Permisos" en Firefox.

Conociendo los **Dispositivos Móviles!**



Conociendo cómo funcionan los **Dispositivos Móviles**

Introducción

Un aspecto que no podía pasar por alto es cómo funcionan los celulares que manejamos hoy en día. Si bien cada día se suman nuevos dispositivos a Internet, el celular ocupa un lugar de privilegio por centralizar en un mismo equipo muchas funciones que antiguamente se realizan con varios dispositivos: fotografiar, filmar, calcular, llamar y un largo etcétera. Hoy un solo dispositivo realiza todo eso y te permite además sumar varias otras funciones o "actividades" a través de las aplicaciones que les instalamos.

Pero como se dice, "si es gratis, pagas con tus datos". Ese *sin costo* tiene indirectamente un pago que son los datos que nosotros generamos a través del uso del dispositivo, permitiendo a las empresas conocernos y realizar segmentación de publicidad por ejemplo.

Actividad:

1. Una buena práctica para mantener seguro tus datos es usar un método de autenticación en el equipo: contraseña / patrón / huella / reconocimiento facial, etc. Si tienes, puedes animarte a cambiarlo, si no cuentas con uno será un buen momento para que tú equipo está más protegido.

2. Lo segundo que debemos tener en cuenta es de qué forma están configuradas las siguientes funciones de nuestros celulares: Wifi – Bluetooht y GPS. Si están activadas sería prudente desactivarlas para que dejen de recopilar información sobre nosotros y sólo utilizarlas en el momento que las necesitemos. Luego, apagarlas ☺

3. Con respecto a las aplicaciones, vamos realizar algunas actividades:
   - Cuenten la cantidad de aplicaciones instaladas por ustedes.
   - Cuenten la cantidad de aplicaciones que ya venían preinstaladas.

- Tomen 5 de las aplicaciones que más usan y tomen nota de los permisos que les han concedido.

Preguntas:

- ¿Qué cantidad de aplicaciones encontraste instaladas en tú celular? ¿Son realmente necesarias todas ellas? ¿Solés revisar qué aplicaciones tenés instaladas? ¿Alguna vez pensaste que tener tantas instaladas podría provocar que tú equipo funcione más lento?
- ¿Solés utilizar las redes sociales desde la aplicación o desde el navegador para acceder a la página? ¿Qué pasaría si alguien encuentra tú equipo y no tiene bloqueo de pantalla? ¿Podrían acceder a todas tus redes o servicios ya logueados?
- ¿Alguna vez consultaste tú historial de Google Maps? Allí figuran todas tus búsquedas que has hecho desde la instalación de la aplicación en tú equipo. **Link**

Consejos:

- Siempre es bueno que todas aquellas funciones que no estamos utilizando sean desactivadas. Sobre todo las que proporcionan información personal como la geolocalización (GPS), el WiFi y el sistema de Bluetooht. De esta manera nuestro equipo no estará diciendo todo el tiempo aquí estoy, esperando noticias nuevas.
- Si pensas en navegar un rato por Internet, te recomendamos instalar y utilizar un navegador diseñado para móviles llamado Firefox Focus el cual evita publicidad y gran número de rastreadores. **Link**
- Sería genial eliminar todas aquellas aplicaciones que no usas y que has encontrado en tus dispositivos. Sobre todo aquellas que soliciten permisos que no corresponden con la actividad que realizan.
- Siempre habrá alternativas más seguras a aplicaciones monopólicas como las de Google. Cambiar de aplicación a una no tan popular evitara que la empresa recolecte tanta información sobre nuestra actividad.

- Aquellxs que usen Android, pueden pensar en utilizar una cuenta de correo para el celular y otra para sus actividades particulares. Así evitaremos que seamos rastreables fácilmente.
- Podemos dejar de descargar tantas aplicaciones y usar el navegador para acceder a las redes sociales o al servicio que necesitemos. De esta manera evitaremos que la aplicación obtenga información sobre nosotros.

pasandodata

Generando conciencia en el uso seguro y responsable de las TIC