# Pasos prácticos para limitar tu huella digital y cuidar tu protección de privacidad digital

Vivimos conectados casi sin darnos cuenta. Cada vez que abrimos una app, aceptamos una cookie o completamos un formulario, dejamos un rastro de información que otras partes pueden recoger, almacenar y, en ocasiones, compartir sin nuestro conocimiento. La sensación de que nuestros datos personales están fuera de control se ha vuelto común, pero tomar medidas para recuperar ese control no requiere ser un experto en tecnología. Con unos cuantos cambios de hábito y la ayuda de herramientas adecuadas, puedes reducir de forma notable tu exposición en internet.

## Revisa y ajusta la configuración de privacidad de tus cuentas

La mayoría de los servicios online ofrecen opciones de privacidad, aunque a menudo vienen configuradas de la forma más permisiva posible. Dedica una tarde a recorrer tus cuentas principales: redes sociales, correo electrónico, almacenamiento en la nube y servicios de streaming. En cada una, busca el apartado de privacidad o seguridad y pregúntate: ¿quién puede ver mis publicaciones?, ¿qué información de mi perfil es pública?, ¿pueden etiquetarme sin mi consentimiento? Ajusta cada opción al nivel más restrictivo que todavía te resulte útil.

Un punto que muchos pasan por alto es el permiso que conceden a aplicaciones de terceros vinculadas a la cuenta. Por ejemplo, esos juegos, tests de personalidad o aplicaciones de edición de fotos que aceptaste hace años pueden seguir accediendo a tu lista de contactos, fotos o ubicación. Revísalos periódicamente y retira el acceso a los que ya no uses o no reconozcas.

## Controla la información que compartes en redes sociales

Las redes sociales son uno de los canales por los que más datos personales se filtran de forma voluntaria. Publicar la foto del billete de avión, la tarjeta de embarque o la nueva dirección puede parecer inofensivo, pero esos datos pueden ser utilizados para suplantar tu identidad o para robos físicos. Como regla general, evita compartir información que pueda usarse para responder preguntas de seguridad típicas (nombre de tu mascota, colegio, fecha de nacimiento).

Otra práctica recomendada es no hacer pública tu ubicación en tiempo real. Publicar que estás de vacaciones lejos de casa es un aviso para posibles intrusos. Espera a compartir las fotos y comentarios cuando hayas regresado. Además, revisa las etiquetas geográficas que las aplicaciones añaden automáticamente a tus imágenes; muchas cámaras y teléfonos insertan los datos de localización en los metadatos de la foto.

## Gestiona las cookies y los rastreadores en tu navegador

Cada sitio web que visitas puede dejar pequeñas marcas llamadas cookies, que registran tu actividad. Algunas son necesarias para que la web funcione (por ejemplo, mantener tu sesión iniciada), pero otras son rastreadores que construyen un perfil de tus intereses para mostrarte publicidad personalizada o vender tu información a terceros.

Puedes empezar por configurar tu navegador para que rechace las cookies no esenciales. La mayoría de los navegadores modernos incluyen un apartado de privacidad donde puedes elegir "solo cookies necesarias" o "rechazar todas". También existen extensiones gratuitas que bloquean rastreadores y anuncios de forma automática. Otra medida eficaz es usar un navegador o un modo de navegación que no guarde el historial ni las cookies después de cerrar la sesión. Combinar estas opciones con un motor de búsqueda que no rastree tus consultas también suma puntos a tu protección de privacidad digital.

## Utiliza contraseñas seguras y autenticación en dos pasos

Una contraseña débil o reutilizada en varios servicios es una de las puertas de entrada más comunes para los ciberdelincuentes. Si un servicio sufre una filtración de datos y tu contraseña queda expuesta, el atacante probará esa misma combinación en otras cuentas. Para evitarlo, crea contraseñas largas y únicas para cada servicio. Un gestor de contraseñas puede generarlas y recordarlas por ti, de modo que solo necesites acordarte de una contraseña maestra.

Además, activa la autenticación en dos pasos (2FA) siempre que esté disponible. Esta capa extra de seguridad exige un segundo código, normalmente enviado a tu teléfono o generado por una aplicación, además de la contraseña. Aunque alguien robe tu contraseña, no podrá acceder sin ese segundo factor. Es uno de los pasos más efectivos para blindar tus cuentas.

## Ejerce tu derecho al olvido y solicita la eliminación de datos

La normativa europea RGPD te otorga el derecho a solicitar que ciertos datos personales sean eliminados de los sistemas de una empresa cuando ya no sean necesarios para la finalidad con la que se recogieron. Si has dejado de usar un servicio o consideras que una empresa conserva información tuya sin motivo, puedes enviar una solicitud de supresión. Muchas plataformas tienen un formulario específico para ello; otras requieren un correo electrónico. Aunque no siempre es inmediato, ejercer este derecho ayuda a reducir tu huella digital.

También es recomendable revisar periódicamente qué cuentas tienes abiertas y cerrar aquellas que ya no utilizas. Cada cuenta inactiva es un punto débil potencial: si el servicio sufre una brecha, tus datos quedarán expuestos aunque tú ya no entres. Antes de cerrar una

cuenta, asegúrate de haber descargado cualquier información que quieras conservar, pues una vez eliminada, puede ser difícil recuperarla.

## Protege tu información en el ámbito laboral y profesional

No solo tu vida personal genera datos; tu actividad profesional también deja rastro. Los perfiles en plataformas como LinkedIn, los currículos colgados en portales de empleo o los comentarios en foros especializados contienen información que puede ser utilizada para campañas de phishing muy dirigidas. Por ejemplo, un atacante que sepa en qué empresa trabajas y qué cargo ocupas puede enviarte un correo falso haciéndose pasar por un compañero o un proveedor.

Para minimizar este riesgo, limita la información visible en tu perfil profesional a lo estrictamente necesario para tu búsqueda de empleo o tu red de contactos. No incluyas tu dirección, teléfono personal ni datos bancarios. Además, utiliza una dirección de correo electrónico específica para cada plataforma profesional, de modo que si una sufre una filtración, las demás no se vean afectadas.

En este contexto, contar con soluciones para proteger tus datos se vuelve indispensable. Herramientas como Meritoo.ai, que ofrecen monitoreo continuo y estrategias personalizadas, permiten detectar a tiempo posibles exposiciones de información sensible y actuar antes de que se conviertan en un problema mayor. Integrar este tipo de recursos en tu rutina digital te da una capa adicional de tranquilidad.

## Mantén actualizados tus dispositivos y aplicaciones

Los hackers buscan constantemente vulnerabilidades en el software que usamos. Cuando los fabricantes lanzan actualizaciones, suelen incluir parches de seguridad que corrigen esos agujeros. Ignorar las actualizaciones de tu sistema operativo, navegador o aplicaciones deja tu equipo expuesto a ataques que podrían haberse evitado fácilmente.

Configura tus dispositivos para que se actualicen de forma automática, al menos en lo que respecta a parches de seguridad. Si prefieres hacerlo manualmente, establece un recordatorio mensual para revisar si hay actualizaciones pendientes. Lo mismo aplica para el firmware de tu router: un router desactualizado puede ser la puerta de entrada a toda tu red doméstica.

La combinación de todos estos hábitos forma una barrera sólida frente a la exposición innecesaria de tus datos personales. No se trata de volverse paranoico, sino de adoptar una actitud consciente y proactiva. Cada pequeño ajuste suma. Y cuando sientas que el proceso es abrumador, recuerda que existen soluciones para proteger tus datos que pueden automatizar parte del trabajo, permitiéndote centrarte en lo que realmente importa: disfrutar de la vida digital con la confianza de que tu información está bajo tu control.