Gestionando su huella digital

La huella digital es toda la información que existe en internet a causa de la actividad en línea. Incluye, aunque sin limitarse a ellas, las publicaciones en las redes sociales, chats, textos, historiales de búsqueda, correos electrónicos, compras en línea y datos de ubicación. Su huella digital puede:

- **Aumentar el riesgo de sufrir estafas.** Los estafadores y timadores pueden utilizar su huella digital para fijarle como objetivo, suplantarle o robarle información.
- **Exponerle a vigilancia, tanto por parte de agencias gubernamentales como de personas que ejercen actividades de control o abusivas.** Incluye saber dónde se encuentra si tiene habilitada la ubicación o si está «pendiente» de sus redes sociales.
- **Aumentar la probabilidad de victimización.** Los criminales utilizan la huella digital de las personas para fijarlas como objetivo y atraerlas hacia situaciones laborales de manera forzosa o bajo coacción. Los miembros de grupos extremistas y otros delincuentes también pueden utilizar la huella digital de la gente para atribuirles mensajes y crímenes de odio.
- **Impactar negativamente en cuestiones de inmigración.** Ahora, las cuentas en redes sociales, nombres de usuario/alias y demás información digital debe ser revelada con respecto a muchas aplicaciones relacionadas con la inmigración, y se podrán examinar dispositivos electrónicos cuando alguien quiera entrar en territorio de los EE.UU. o esté bajo custodia del Departamento de Seguridad Nacional. La actividad en línea de las personas se puede utilizar para influir en la decisiones relacionadas

con su detención, deportación, ajuste de estatus, nacionalización, asilo o cualquier otra forma de ayuda a la inmigración.

¡La gestión de su huella digital es crítica para su seguridad y su reputación!

12 Consejos para la gestión de su huella digital

1. **Proteja sus dispositivos y cuentas.** Compruebe que todos sus dispositivos tengan una contraseña segura, preferiblemente con autentificación en dos pasos. La autentificación en dos pasos se produce cuando existen dos métodos de autentificación, como una contraseña más la introducción de un código recibido en su teléfono móvil.

2. **No comparta información privada.** No publique su nombre completo, dirección, número de teléfono u otra información privada en internet, incluyendo las redes sociales.

   No etiquete su ubicación en las redes sociales.

   No publique fotos que puedan identificar dónde está, dónde vive, dónde trabaja o va a la escuela, como números de portal, letreros con nombres de calles, matrículas, logotipos de uniformes, etc.

3. **Cree cuentas privadas.** Si tiene cuentas de reuniones sociales, asegúrese de que sean privadas. En general, se puede hacer yendo a su cuenta, accediendo a Ajustes o a Privacidad y asegurándose de seleccionar la opción «privada».

4. **Elimine cuentas antiguas.** Si ya no utiliza una cuenta, elimínela. Análogamente, desactive el almacenamiento en la nube o las cuentas en dispositivos antiguos que aún conserve pero que apenas utilice.

5. **Desactive la ubicación.** Para desactivar la ubicación en un dispositivo, vaya a los ajustes de dicho dispositivo, que suele encontrarse en «Privacidad», «Seguridad» o «Ubicación». Desde allí, desactive los Servicios de Ubicación para que las aplicaciones y servicios no conozcan su ubicación.

6. **Limite lo que publica.** Publique una cantidad mínima de datos en línea.

   Tenga cuidado con lo que publica, ya que podría ser malinterpretado o

podría aumentar su riesgo de exposición. Por ejemplo, si publica una foto bebiendo alcohol, sosteniendo un arma, etc.

7. **No acepte solicitudes de amistad de gente a la que no conoce.** Asegúrese de aceptar únicamente solicitudes de amistad de gente a la que conoce. Cualquiera puede esconderse detrás de un perfil, incluyendo estafadores, traficantes y gente que intenta vigilarle. Elimine de sus cuentas a aquellos amigos a lo que no conozca personalmente.

8. **Elimine material y aplicaciones sensibles de sus teléfonos y demás dispositivos.** Si viaja a otros países, los agentes del Departamento de Seguridad Nacional podrían buscar en sus dispositivos electrónicos en los puntos de entrada a su vuelta a los EE.UU. Elimine cualquier texto, foto, aplicaciones y demás material que pueda ser malinterpretado.

9. **Comuníquese de forma segura.** Utilice aplicaciones de mensajería que ofrezcan cifrado de extremo a extremo como WhatsApp, Signal o Telegram.

   Nota: Aunque son más seguras, incluso las plataformas con mensajes cifrados pueden contribuir a su huella digital mediante el almacenamiento de metadatos, por ejemplo con quién se comunica y cuándo, además de contenido compartido como vídeos, imágenes o información de perfil. Tenga cuidado con lo que comparte.

10. **Tenga cuidado al navegar en la red.** No haga clic en enlaces sospechosos de remitentes a los que no conoce ni visite sitios web que no sean de confianza, ya que podrían exponerle a virus y a posible vigilancia.

    Proporcione únicamente la información necesaria, y tenga mucho cuidado con los sitios web y las aplicaciones que le pidan más información personal de la necesaria.

    Elimine periódicamente las cookies de su navegador y de su caché. Normalmente puede hacerlo yendo a los Ajustes de su navegador, después a los Ajustes de Privacidad y accediendo a «limpiar datos de navegación» u opción similar.

11. **Utilice un teléfono móvil temporal o desechable.** Estos teléfonos suelen ser de prepago y no están atados a un contrato, por lo que son más fáciles de usar de forma anónima para evitar ser rastreados. No obstante, si utiliza un teléfono temporal, asegúrese de que la gente que tenga que contactar con usted (trabajadores sociales, abogados, etc.) tengan su número actualizado.

A veces la gente decide tener dos teléfonos: uno temporal para su actividad en línea y uno permanente para mantener una comunicación importante y estable con la gente importante.

12. **Tape las cámaras.** Cubra las cámaras de los teléfonos y portátiles para bloquear la lente mientras no la esté utilizando. Así evitará que invadan su privacidad.