Reglas básicas para la seguridad digital

Si quieres navegar y relacionarte de manera segura en cualquier entorno digital, ya sea en un sitio web, una aplicación, un videojuego en línea o una red social, estas cinco reglas te serán muy útiles.

Las 5P de la seguridad digital

Palabra clave	Regla básica
Perfil	No compartas **información personal** a través de la Red.
Privacidad	Revisa los **filtros de privacidad** de las herramientas que utilices.
Protección	No uses **contraseñas** evidentes como *123456* o *contraseña*. Ten cuidado con las redes WIFI públicas.
Positividad	Mantén un **tono amable**, respetuoso y positivo.
Permiso	Comprueba las **licencias** y asegúrate de tener **permisos** para compartir lo que publicas.

Recomendaciones para una navegación privada y segura

Toma nota de estas siete recomendaciones para proteger tu identidad y tus datos en Internet.

1. Navega de forma privada

Usa la opción de navegación privada y utiliza un alias o *nickname* en los sitios no oficiales.

La mayoría de los navegadores disponen de un modo de navegación privada o de incógnito. Esto te permite navegar sin guardar los datos de las páginas visitadas, las sesiones iniciadas ni otros datos temporales. Si necesitas registrarte en un sitio web de autoría desconocida, usa un alias para proteger tu identidad.

2. Borra tus datos de navegación

Limpia las *cookies* y el historial de navegación.

Las *cookies* son ficheros de datos sobre tu actividad que se almacenan en el navegador. Igual que los sitios visitados, las *cookies* permiten agilizar la navegación, aunque también pueden recoger información sensible sobre tus hábitos. Borra periódicamente el historial y las *cookies* de tu navegador para ceder solo los datos necesarios. Usar el modo de navegación privada también es una solución.

3. Protege tu privacidad

Cierra sesión al terminar. Ajusta las opciones de privacidad del navegador y revisa las políticas de privacidad de los sitios que visites.

Recuerda que, al cerrar la ventana del navegador, las sesiones que hayas iniciado (en tu cuenta de correo, en una red social o en cualquier tipo de perfil privado) seguirán abiertas. Asegúrate de cerrar sesión desde la propia página o aplicación antes de salir del navegador. Asimismo, consulta las políticas de privacidad y configura los ajustes necesarios para reducir los datos que compartes y evitar que rastreen tu perfil de usuario.

4. Limítate a instalar lo esencial

Ten en cuenta que las barras de herramientas y otros *plug-ins* almacenan información.

Los *plug-ins* son extensiones de un programa, una aplicación web o un navegador que amplían alguna función. Instala solo aquellos que sean necesarios y descárgalos de sitios fiables. Los *plug-ins* almacenan información sobre la navegación, y los piratas informáticos pueden utilizarlos para robarte datos importantes.

5. Preserva tu intimidad

Asegúrate de tener la *webcam* apagada.

Configura los permisos de acceso a la cámara y al micrófono de tu teléfono móvil, ordenador o cualquier otro de dispositivo conectado a la Red para evitar que te vean o escuchen sin tu autorización.

6. Elimina información personal

Borra los metadatos de lo que publiques en Internet.

Cualquier archivo que publiques (imagen, vídeo, pódcast, documento…) contiene información que puede comprometer tu privacidad. Antes de publicar cualquier fichero, recuerda acceder a las propiedades del archivo y eliminar metadatos como la fecha y la hora en que se creó, tu nombre o la ubicación.

7. Conéctate a redes seguras

Recuerda que al usar una WIFI pública tus datos son más vulnerables.

Las redes WIFI públicas o gratuitas, al no requerir contraseña o dar acceso (aun con contraseña) a muchas personas usuarias, son redes desprotegidas que ponen en serio riesgo tus datos. Evita conectarte a este tipo de redes y, si lo haces, no inicies sesión en cuentas privadas ni realices trámites que puedan exponer datos confidenciales, como tu firma digital o tu información bancaria.

Recomendaciones para usar las redes sociales de forma privada y segura

Haz de las redes sociales una herramienta segura, tanto para ti como para tus contactos, siguiendo estos consejos.

1. Oculta tus datos

Configura tu perfil de forma que no sean públicos aquellos datos que no quieres que sean accesibles para los buscadores.

Al crear un perfil en una red social se dan muchos datos personales (nombre, apellidos, fecha de nacimiento, lugar de residencia, número de teléfono…) fácilmente accesibles para los buscadores. Ajusta las opciones de privacidad de tus perfiles sociales para mantenerlos ocultos y proteger tu identidad.

2. Usa contraseñas seguras

Utiliza contraseñas adecuadas y que no puedan adivinarse fácilmente.

Infórmate sobre la creación de contraseñas seguras, que contengan símbolos, cifras y letras, mayúsculas y minúsculas. Evita usar palabras o conceptos predecibles (el nombre del lugar donde vives, tu fecha de nacimiento…) y crea una contraseña nueva para cada servicio que necesites. Usar un gestor de contraseñas, con una sola clave maestra, puede serte útil.

3. Pide permiso

Respeta los derechos ajenos y no difundas contenidos de terceras personas sin su consentimiento.

Es habitual creer que porque un contenido (una foto, un texto, un vídeo…) está en la Red puede usarse libremente. Respetar los derechos de las personas a la hora de difundir contenido ajeno es fundamental: se debe pedir permiso y, en caso de tenerlo, citar la autoría. Esto es aún más importante a la hora de compartir contenido privado, como una nota de voz o el fragmento de una conversación.

4. Exponte lo mínimo

Ten cautela a la hora de publicar información personal: evita dar demasiados detalles.

En las redes sociales puedes llegar a compartir tu vida prácticamente en directo. Esto supone que cualquiera puede saber dónde estás, con quién, qué haces y cuándo. Procura limitar al máximo este tipo de información en tus publicaciones por tu propia seguridad y la de tus acompañantes. Recuerda, además, que todas las redes sociales permiten tener el perfil privado, de modo que solo las personas que elijas puedan acceder a lo que publicas.

Recomendaciones para proteger tus servicios de mensajería

Sigue estas recomendaciones para proteger tus mensajes y dispositivos al usar el correo electrónico.

1. Usa servicios fiables

Utiliza servicios de correo de confianza, como Gmail, Outlook, etc.

Al crear tu cuenta de correo con una empresa consolidada, tienes más garantías de seguridad y de que funcione correctamente. Además, tu dirección de correo es percibida como de confianza, de manera que es menos probable que tu mensaje se considere no deseado y no llegue a ser leído.

2. Crea una segunda cuenta

Usa una segunda cuenta para registrarte en servicios comerciales o de interés temporal.

Es recomendable tener una cuenta alternativa para mantener la cuenta principal libre de correo no deseado, listas de correo y publicidad. De esta manera, también proteges tu privacidad. Asimismo, existen servicios de correo temporal, en los que puedes crear direcciones de un solo uso para un registro o transacción puntual.

3. Si dudas, no lo abras

No abras correos dudosos ni descargues imágenes por defecto.

Desconfía de los nombres de remitentes desconocidos y de los asuntos sospechosos o llamativos. Si el nombre del remitente te resulta familiar, comprueba la dirección de correo. En caso de duda, no pulses nunca en ningún enlace ni descargues imágenes o documentos adjuntos. Marca el correo como no deseado y elimínalo de tu buzón.

4. Protege a las personas destinatarias

Utiliza "Con copia oculta" (CCO) cuando mandes correos a muchas personas.

Evita mandar correos masivos, ya que pueden ser considerados no deseados por los servicios de mensajería de quienes los reciban. Aun así, si necesitas incluir a varias personas en un mismo mensaje, ocúltalas para proteger sus direcciones de correo, especialmente si no se conocen entre sí.

5. Haz limpieza de datos

Borra periódicamente los registros y ficheros de las conversaciones mantenidas.

Mantén limpia tu bandeja de entrada y tus archivos. Conserva solo los mensajes necesarios, imprime o guarda los que consideres y borra toda la información en línea que pueda comprometer tu privacidad. Vacía la papelera para eliminar definitivamente los archivos que ya no quieras.