# NORMAS DE SEGURIDAD PARA NAVEGACION

## Regla 1: Descarga desde sitios web seguros

En algunas ocasiones hemos tenido la necesidad de descargar un documento o algún programa importante que deseamos o que nos sugieren, entonces debemos averiguar la procedencia del sitio web, su reputación para tener la confianza de hacerlo. Así nos aseguramos estar bajando el programa realmente lo deseado y no algún software que busque hackearnos.

## Regla 2: No compartir nuestros datos bancarios

Muchos atacantes informáticos ven en tus datos bancarios el botín perfecto, por ello es necesario no brindar tu información bancaria en internet bajo ningún punto de vista, salvo el caso que tú ya conozcas la seriedad de una empresa, su reputación y su experiencia, porque quizá tengas que hacer alguna adquisición. No obstante es mejor utilizar las plataformas de pagos seguras como Paypal.

## Regla 3: Ten cuidado al navegar desde tu móvil

Si tu ya está tomando las precauciones del caso al navegar desde tu PC de escritorio o portatil, no te olvides de tu móvil, pues es muy importante que tengas en cuenta las mismas reglas para este caso. A través de los dispositivos como smartphones, los dueños de los ajeno tienen mayor probabilidades de vulnerar elementos de seguridad que quizá te brinde tu sistema operativo.

## Regla 4: Borrar las cookies

Una cookie es un archivo creado por un sitio web que contiene pequeñas cantidades de datos y que se envían entre un emisor y un receptor, con la finalidad de conocer las preferencias del usuario y que su experiencia en el sitio se facilite. Sin embargo la información que se comparta es susceptible de llegar a terceros por lo que conviene valorar el tráfico de estos datos y en todo caso desde el navegador podemos decidir borrar dichas cookies para evitar sustos innecesarios.

## Regla 5: Restringe tu información en redes sociales

Toda la información que subimos a las redes sociales es de dominio público, a pesar de que lo compartamos supuestamente para una cierta área de amigos. Si compartimos datos innecesarios como direcciones de casa, teléfonos, correos, estamos expuestos a muchos peligros, por ello usa de manera responsable las redes sociales para evitar chantajes o cosas peores.

## Regla 6: Crea contraseñas seguras para cada una de tus cuentas

Al crear una contraseña segura evitarás que alguien pueda acceder a tu correo, redes sociales o cuentas de usuarios de los servicios online que utilizamos normalmente. Como sabemos muchas de ellas vinculas datos de tu móvil o tarjetas bancarias, entonces se hace indispensable crear contraseñas que nadie se las imagine. Te doy un consejo: crea una contraseña entre números, letras minúsculas y mayúsculas, caracteres del teclado, barra espaciadora, en fin; pero jamás con algo que tenga que ver con tu nombre o el nombre de algún familiar o el sitio de trabajo o algo que te rodee. Luego cópiala a mano en una libreta física, tenla siempre a la mano y de allí digita en tus cuentas online. Así tendrás toda la seguridad del mundo.

## Regla 7: Siempre utilizar un antivirus

Si por descuido abriste un enlace no apto y enseguida ingresó por la red un virus que pone en riesgo to ordenador, pues déjame decirte que estás en problemas. Para empezar y al momento de instalar tu sistema operativo en tu PC o Celular, debes inmediatamente contratar un servicio antivirus, o al menos uno gratis y así evitar ser víctima de robo de información o mucho peor. Si ya estás infectado existen algunos antivirus que pueden ayudarte a eliminar los archivos dañados, pero ni siempre ocurre así.

## Regla 8: Abre enlaces de fuentes conocidas

Cuando abrimos enlaces de fuentes desconocidas las probabilidades de ser infectado nuestro ordenador son casi el 100%, es por eso que debemos evitar al máximo abrir enlaces desde foros de internet, foros de chat, plataformas como Facebook, entre otras. Siempre procuremos abrir enlaces de fuentes conocidas. Se nota cuando un sitio tiene buena reputación o no, desde su diseño.

## Regla 9: Las zonas Wi-fi públicas gratis suelen ser inseguras

Los mismos teléfonos inteligentes detectan cuando una conexión no es segura y nos advierten, de modo que es preferible utilizar nuestros propios datos si realmente queremos hacer una acción o mejor si tenemos nuestro dispositivo bien guardado.