Las contraseñas se utilizan para que solamente las personas que estén autorizadas puedan acceder a una determinada información o servicio. Por este motivo es muy importante asegurarse de utilizar contraseñas seguras. Enseguida se enlistan algunas buenas prácticas para la gestión y uso de contraseñas seguras.

- **Las contraseñas son personales y no se deben compartir.**

Las contraseñas son confidenciales. Por lo tanto, se debe tomar en cuenta los siguientes aspectos:

1. No se deben apuntar en un papel, en un tablón, debajo del teclado o en un post-it.
2. No se deben difundir o comunicar a través de un medio inseguro.
3. Cuando nos proporcionan una contraseña es únicamente para nosotros, ya que seremos los responsables de su uso.

- **No debemos usar las contraseñas por defecto.**

Nunca se deben usar las contraseñas por defecto o que nos haya proporcionado por primera vez, siempre se deben cambiar lo más pronto posible.

- **Las contraseñas utilizadas tienen que ser robustas, seguras, impersonales y no se deben reutilizar.**

Las contraseñas que utilicen tienen que tener las siguientes características:

1. La longitud mínima recomendable de una contraseña es de 8 caracteres.
2. Estos 8 caracteres tienen que incluir mayúsculas, minúsculas, números y caracteres especiales como por ejemplo * (# @, etc.
3. Deben ser impersonales. No se deben usar nunca contraseñas como el cumpleaños de una persona, el nombre de algún familiar, números de teléfono, etc.
4. No se debe repetir la misma contraseña para distintos servicios. En cada uno de los servicios se tienen que usar contraseñas distintas.

- **Las contraseñas se tienen que cambiar periódicamente.**

Existen filtraciones, vulnerabilidades y multitud de situaciones en que una contraseña puede quedar expuesta. Por lo tanto, es recomendable que periódicamente se vayan modificando las contraseñas de los servicios que utilizan.

- **Usar equipos de confianza para acceder a servicios críticos.**

Hay que usar un equipo seguro para acceder a un servicio que sea crítico. Evitar usar equipos públicos que se pueden encontrar en cibercafé, bares, bibliotecas, hoteles, etc. El riesgo que un equipo público esté comprometido es mucho más elevado que en un equipo que es de nuestra confianza.