



EMPLEADOS

# Contraseñas

básico



### No utilizar las contraseñas por defecto.

Cambias las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones y sistemas.



### Doble factor de autenticación (2FA).

Incorporar sistemas de autenticación multifactor en los accesos a servicios siempre que sea posible. Es una capa de seguridad extra.



### No compartir las contraseñas con nadie.

Mantienes en secreto tus claves y evitas compartirlas.



### Las contraseñas deben de ser robustas.

Generas tus contraseñas teniendo en cuenta su fortaleza.



### No utilizar la misma contraseña para servicios diferentes.

Te aseguras de elegir distintas contraseñas para cada uno de los servicios que utilizas.



### Cambiar las contraseñas periódicamente.

Haces que se modifiquen las contraseñas cada \_\_\_\_\_.



### No hacer uso del recordatorio de contraseñas.

No utilizas nunca las opciones de recordatorio de contraseñas de navegadores y aplicaciones.



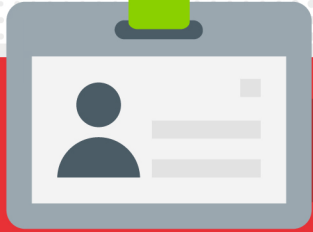
### Utilizar gestores de contraseñas.

Usas gestores de contraseñas seguros para poderlas recordar.



### Ciberllave o Passkey.

Asegurar la información con el uso de ciberllave o passkey en las plataformas que lo permitan.



EMPLEADOS

# Contraseñas

avanzado



## ***Gestión de contraseñas.***

Defines un sistema de gestión de contraseñas avanzado que contempla todos los aspectos relativos a su ciclo de vida.



## ***Técnicas de autenticación externas.***

Consideras la utilización de sistemas de autenticación externos descentralizados.



## ***Herramientas para garantizar la seguridad de las contraseñas.***

Te ayudas de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas.