CONTRASEÑAS
Buenas prácticas en el uso de las contraseñas

Seguir una serie de recomendaciones de seguridad en el uso de contraseñas reducirá el riesgo de que los ciberdelincuentes consigan acceso a los sistemas de la empresa.

Robustez

La complejidad de las contraseñas es una de las principales medidas de seguridad. Usar contraseñas simples supone un riesgo, ya que los ciberdelincuentes pueden adivinarlas muy rápido. Contraseñas basadas en un nombre o el comúnmente usado 123456 son descubiertas en segundos. Consejos:

- **Longitud mínima de 8 caracteres**, puesto que cuanto más larga sea esta, más tiempo se tardará en descubrirla.
- Utilizar combinaciones de letras **mayúsculas, minúsculas, números y símbolos.**

Una forma de conseguir contraseñas robustas es utilizar **reglas nemotécnicas** aplicadas a una frase:

- Seleccionamos una frase: «**en un lugar de la mancha**».
- Hacemos uso de mayúsculas: «**En un lugar de la Mancha**».
- Incluimos el servicio: «**En un lugar de la Mancha Correo**».
- Añadimos números: «**En un lugar de la Mancha Correo de 2019**».
- Añadimos caracteres especiales: «**En un lugar de la Mancha Correo de 2019!**».
- La comprimimos utilizando la primera letra de cada palabra: «**EuldlMCd2019!**».

NOTA: La forma más segura de obtener una contraseña robusta es utilizar un generador de contraseñas que nos permita elegir la longitud, el tipo de caracteres, etc.
No obstante, cuanto más complejas sean mayor será la dificultad para recordarlas.
Por ello, lo más recomendable es utilizar un gestor de contraseñas y así solo tener que recordar y conservar la clave maestra, la que abre dicho gestor.

No tener una compartida

La contraseña debe ser intransferible y nadie bajo ningún concepto debe saber cuál es. Si otra persona conocedora de tu contraseña hiciera algo con tus credenciales de acceso, podrías ser responsable.

No usar la misma

Utilizar la misma clave para acceder al correo electrónico, redes sociales, tiendas online, etc., no es una práctica segura. Cada servicio debe tener su propia contraseña de acceso.

Doble factor de autenticación

Esto se consigue por medio una nueva clave que, generalmente, es de un solo uso. Normalmente, este segundo factor de autenticación está vinculado a un teléfono móvil, por medio de una aplicación específica.