

CIBERCONSEJOS PARA CREAR

CONTRASEÑAS SEGURAS

Los ciberdelincuentes se sirven de diversas técnicas y herramientas con las que atacar a nuestras contraseñas. Los usuarios no siempre les dificultamos esta tarea, y solemos caer en malas prácticas que ponen en peligro nuestra seguridad



1. QUE TU CLAVE TENGA UNA EXTENSIÓN DE, AL MENOS, 9 CARACTERES.
2. UTILIZAR MAYÚSCULAS, MINÚSCULAS, NÚMEROS Y CARACTERES ESPECIALES (PUNTOS Y SÍMBOLOS).
3. UTILIZA FRASES DE CANCIÓN, POEMA, CITA, PELÍCULA O PASAJE DE UN LIBRO.
4. UTILIZA SECUENCIA DE PALABRAS INCONEXAS (CON REGLAS DE MAYÚSCULA/MINÚSCULA INCLUIDA).
5. UTILIZA TRES PALABRAS BAJO LA SECUENCIA "PERSONA", "ACCIÓN" Y "OBJETO" (CON REGLAS DE MAYÚSCULA/MINÚSCULA INCLUIDA).



AL CREAR UNA CLAVE **NUNCA**:

1. UTILIZAR EL NOMBRE, O EL NOMBRE DE ALGÚN FAMILIAR.
2. UTILIZAR EL NOMBRE DE ALGUNA MASCOTA.
3. UTILIZAR FECHAS DE CUMPLEAÑOS
4. USAR DIRECCIONES DEL TRABAJO O DOMICILIO PARTICULAR
5. USAR EL RUT PERSONAL O DE ALGÚN FAMILIAR
6. USAR EL NÚMERO DE TELÉFONO



1. UN EJEMPLO DE CONTRASEÑA SEGURA ES LA UTILIZACIÓN DE UNA FRASE QUE SEA FÁCIL DE RECORDAR, EJ:
CREANDO MI CLAVE SEGURA
2. CUANDO TENGAMOS NUESTRA FRASE LA MODIFICAMOS PARA HACERLA MÁS ROBUSTA Y LA REEMPLAZAMOS LOS ESPACIOS POR SÍMBOLOS:
CREANDO_MI_CLAVE_SEGURA
3. LUEGO PODEMOS AGREGAR MAYÚSCULAS:
CREANDO_MI_CLAVE_SEGURA
4. TAMBIÉN PODEMOS REEMPLAZAR VOCALES POR NÚMEROS:
CR34ND0_M1_CL4V3_S3GUR4



CURIOSIDAD:

SI ES POSIBLE, LOS USUARIOS DEBEN ELEGIR CONTRASEÑAS DE 10 CARACTERES QUE INCLUYAN NÚMEROS O SÍMBOLOS. DE ESTA MANERA SE CREAN 171.3 TRILLONES (1.71 X 1020) DE POSIBILIDADES. CON UN PROCESADOR DE GPU QUE PRUEBE 10,3 MIL MILLONES DE HASHES POR SEGUNDO, DESCIFRAR LA CONTRASEÑA LLEVARÍA APROXIMADAMENTE 526 AÑOS.



EN CASO DE SER VÍCTIMA DE UN FRAUDE
DENUNCIA 24hrs.



(+562) 2486 3850



www.csirt.gob.cl

