

CONTRASEÑAS SEGURAS

¿QUÉ DEBO TENER EN CUENTA?



* * * *

01. Longitud

Cuanto más larga, mejor. Intenta crear contraseñas con al menos 12 caracteres.

02. Complejidad

Mezcla letras (mayúsculas y minúsculas), números y caracteres especiales. No uses palabras comunes ni patrones.

🔒 Password Protected

EL2S454896B*



03. Evita información personal

No uses información personal fácilmente disponible, como tu nombre, fecha de nacimiento o nombres de familiares.

04. No uses contraseñas comunes

No uses la misma contraseña para diferentes cuentas. Si una se ve comprometida, las demás seguirán seguras.



05. Actualización regular

Cambia tus contraseñas de forma regular, especialmente si sospechas de alguna actividad sospechosa.

06. Seguridad

Si necesitas escribir tu contraseña en papel o en algún documento, no la dejes en tu computadora ni en tu escritorio. Asegúrate de guardar estas contraseñas en un lugar secreto o bajo llave.



07. Cifrado de documentos

- *Abrir el documento que se va a cifrar
- *Clic en "Archivo"
- *Clic en "Proteger documento"
- *Clic en "Cifrar con contraseña"
- *Asignar una contraseña segura y que recuerdes (si se pierde la contraseña, el archivo no se puede recuperar)

Protección de datos

Fma nieves

Protecciondatos@fmanieves.org

01



Según el Decreto 1377:2013, las empresas solo deberán recolectar aquellos datos que sean pertinentes y adecuados para realizar sus actividades.

02



Las empresas deben solicitar la autorización al titular para tratar sus datos, además de explicarle para qué serán utilizados.

05

MARCO LEGAL

*Art. 15 de la Constitución Política 1991

*Ley 1266 de 2008

*Ley 1273 de 2009

*Sentencia C748/11

*Ley 1581 de 2012 (Ley general)

*Resolución 76434 de 2012

*Decreto 1377 de 2013

*Decreto 886 de 2014

*Decreto 1074 de 2015



AUTORIZACIÓN DEL TITULAR

Decreto 1377:2013

Sabías que las empresas necesitan tu autorización para realizar el tratamiento de tus datos personales?

03

Las empresas deben conservar prueba de que el titular autorizó el tratamiento de sus datos. Por otra parte, el titular tiene derecho a anular su autorización de manera gratuita.



04

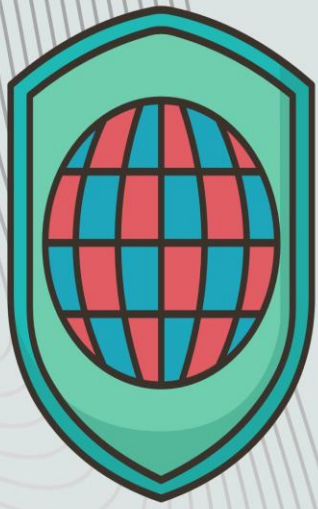


Para que la autorización del titular sea válida, debe ser expresa, informada, previa, explícita e inequívoca. Puede ser oral y/o escrita.

FMA NIEVES

PROTECCIÓN DE DATOS

protecciondatos@fmanieves.org



PROTEGE TUS DATOS

Consejos de Ciberseguridad

01 UTILIZA CONTRASEÑAS SEGURAS

Largas, complejas y únicas para cada cuenta. Usa una combinación de letras, números y símbolos.



02 MANTÉN TUS DISPOSITIVOS ACTUALIZADOS

Las actualizaciones a menudo incluyen mejoras de seguridad importantes.

03 EVITA CONECTARTE A REDES WIFI PÚBLICAS

Mejor utiliza una red privada virtual (VPN) para mantener tu información segura.



04 NO REVELES INFORMACIÓN PERSONAL

Tus datos personales pueden usarse para el robo de identidad.

05 HAZ COPIAS DE SEGURIDAD

Realiza copias de seguridad con frecuencia en un disco duro externo.



MEDIDAS DE SEGURIDAD

FISICAS

1

OFICINA

Tu oficina, habitación y/o archivero deben estar bajo llave. La llave también debe estar en un lugar seguro y restringido.



DOCUMENTOS

Deben estar organizados y almacenados en lugares con condiciones seguras (no humedad, no sol, buena ventilación, poco riesgo de inundación o incendio)

2



USB Y DISCOS EXTRAÍBLES

Haz copias de seguridad en discos extraíbles o USB y guardarlos en lugares seguros.

3

