BUENAS PRÁCTICAS EN CIBERSEGURIDAD

CUIDADO CON LOS CORREOS

No abrir **enlaces ni descargar archivos de remitentes desconocidos.**

Los correos de phishing a menudo incluyen enlaces falsos que dirigen a páginas fraudulentas diseñadas para robar contraseñas. Implementar soluciones antiphishing ayuda a identificar y bloquear estos intentos.

CONTRASEÑAS SEGURAS

Crear contraseñas complejas **(mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos)** para prevenir accesos no autorizados.

Los gestores de contraseñas permiten crear y almacenar contraseñas seguras sin tener que recordarlas todas.

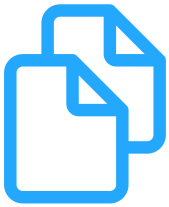
Además, **activar el doble factor de autenticación (2FA)** proporciona una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado al teléfono móvil.

ACTUALIZACIONES PERIÓDICAS:

Mantener **actualizados los sistemas operativos**, aplicaciones y antivirus garantiza que se instalen parches de seguridad importantes **para corregir vulnerabilidades** que los atacantes pueden explotar.

EVITAR REDES WI-FI PÚBLICAS

Las redes Wi-Fi públicas **no son seguras**, lo que facilita los ataques. Si es necesario usarlas, se debe usar **una VPN** (Red Privada Virtual), que cifra la conexión a Internet y protege la información transmitida.



COPIAS DE SEGURIDAD

Hacer **copias de seguridad frecuentes** de todos los datos importantes y almacenarlas de forma segura, idealmente en un sistema en la nube o en un servidor externo.

CONTROL DE ACCESO Y CUFRADO DE COMUNICACIONES.

Implementar políticas de acceso basadas en roles para que solo el personal autorizado pueda acceder a información confidencial y utilizar cifrado de extremo a extremo en todas las comunicaciones.

ILUSTRE COLEGIO
DE LA ABOGACÍA
DE MADRID