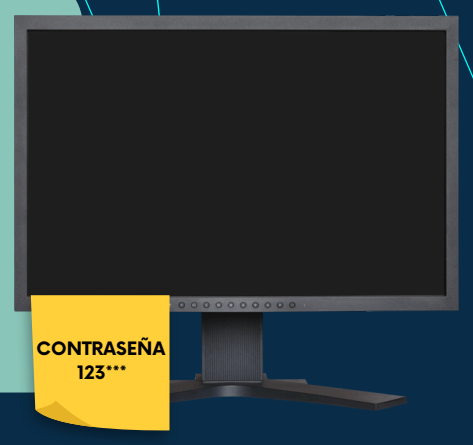
PRÁCTICAS CIBERSEGURAS PARA LOS EMPLEADOS

GIC (Gestión e Investigación en Ciberseguridad)
Lines - UTN La Plata

01 NO EXPONGAS TUS CONTRASEÑAS

Evita anotarlas en papel o dejarlas visibles en tu escritorio. Usa un gestor de contraseñas y crea claves únicas y seguras para cada cuenta, especialmente en servicios críticos como correos y bancos.



02 BLOQUEA TU COMPUTADORA

Cuando te alejes, bloquea tu sesión con Windows + L o desde el menú. No uses equipos o redes públicas para acceder a información sensible y cierra la sesión al terminar tu jornada laboral.

03 DESCARGA SOLO LO NECESARIO

Instala software solo de sitios oficiales y revisa sus permisos antes de usarlo. Si es posible, pruébalo antes para evitar riesgos en la red de tu empresa.

04 CUIDADO CON LOS CORREOS SOSPECHOSOS

No abras mensajes con remitentes desconocidos, errores ortográficos o enlaces sospechosos. Verifica siempre la dirección del remitente y la autenticidad del contenido antes de hacer clic.

05 RESPETA LAS POLÍTICAS DE SEGURIDAD

Sigue las políticas internas para proteger accesos, gestionar contraseñas y realizar copias de seguridad. La seguridad digital es una responsabilidad compartida. Adoptar estas prácticas refuerza la protección de la información y la integridad de los sistemas en el entorno laboral.