



·CAFÉ·
**LA FLOR DE
CÓRDOBA**
DESDE 1938

Ciberseguridad en la empresa

Introducción a la Ciberseguridad: La ciberseguridad es fundamental para proteger la información, las redes y los sistemas de tu empresa de amenazas externas e internas. Es responsabilidad de todos los empleados garantizar la seguridad de los datos y las operaciones. A continuación, te proporcionamos los conceptos básicos de ciberseguridad que debes conocer y aplicar en tu trabajo diario.

1. Contraseñas Seguras:

Una de las primeras líneas de defensa en la ciberseguridad es una contraseña segura. Las contraseñas deben ser únicas, largas y complejas. Evita usar contraseñas fáciles de adivinar, como tu nombre, fecha de nacimiento o palabras comunes.

- Consejos para crear una contraseña segura: Usa al menos 12 caracteres.
- Combina letras (mayúsculas y minúsculas), números y símbolos.
- No reutilices la misma contraseña en múltiples cuentas.
- Cambia tu contraseña regularmente.

Importante: Nunca compartas tu contraseña con nadie, incluso si la solicitud parece legítima. La empresa nunca te pedirá tu contraseña por teléfono o correo electrónico.



Inicia sesión con tu cuenta

Usuario

sistemas

Contraseña

[¿Olvidó su contraseña?](#)

☒ Recuérdame

Iniciar sesión

Iniciar sesión

[¿Olvidó su contraseña?](#)

2. Phishing:

El phishing es un intento fraudulento de obtener información confidencial, como contraseñas y números de tarjetas de crédito, mediante el uso de correos electrónicos, mensajes de texto o sitios web falsos que se hacen pasar por fuentes legítimas.

Cómo identificar un ataque de phishing:

Revisa siempre el remitente del correo electrónico.

- Desconfía de los mensajes que te solicitan información personal o financiera urgente.
- No hagas clic en enlaces ni descargues archivos de fuentes desconocidas.
- Verifica la URL de cualquier sitio web antes de ingresar tus credenciales..

Recuerda: Si tienes dudas sobre la autenticidad de un mensaje, no hagas clic en ningún enlace y contacta al soporte de IT de la empresa.



3. Uso Seguro de Dispositivos Móviles:

Los dispositivos móviles, como teléfonos y tabletas, también pueden ser un objetivo para los ciberdelincuentes. Debes protegerlos con contraseñas o métodos biométricos y seguir prácticas seguras cuando accedas a la red corporativa.

Consejos:

- Bloquea tu dispositivo con una contraseña, patrón o huella digital.
- No descargues aplicaciones de fuentes no confiables.
- Conéctate solo a redes Wi-Fi seguras y evita las redes públicas para realizar tareas sensibles.
- No dejes el teléfono a la mano en barra o mostrador.

Recuerda: Si pierdes tu dispositivo o sospechas que ha sido robado, informa de inmediato al departamento de IT para que se tomen las medidas necesarias.



Inicia sesión con tu cuenta

Usuario

sistemas

Contraseña

[¿Olvidó su contraseña?](#)

☒ Recuérdame

Iniciar sesión

Iniciar sesión

[¿Olvidó su contraseña?](#)

