



Ingoude Company

SEGURIDAD DIGITAL

COMUNIDAD HIJAS DE MARIA AXILIADORA

Start It Now



INTRODUCTION



Ingoude Company



SEGURIDAD DIGITAL

La seguridad digital es el conjunto de medidas y prácticas que se utilizan para proteger la información y los dispositivos electrónicos frente a amenazas como el robo de datos, fraudes y ataques informáticos. Su objetivo es garantizar la privacidad, la confidencialidad y el uso seguro de la información en internet. En un mundo cada vez más conectado, la seguridad digital es fundamental para proteger nuestra vida personal, académica y laboral.



CONCEPTOS DE CYBER SEGURIDAD EFECTIVOS:

CONTRASEÑAS SEGURAS:

Contraseñas seguras:
Claves creadas con letras,
números y símbolos que
dificultan el acceso no
autorizado a la cuenta.

VERIFICACION EN 2 PASOS :

Medida de seguridad adicional
que solicita un código extra,
además de la contraseña, para
ingresar al correo.

INFORMACION CONFIDENCIAL:

Datos privados o sensibles
de la institución que deben
protegerse y no compartirse
sin autorización.

CERRAR SESION EN DISPOSITIVOS COMPARTIDOS :

Medida para evitar que otras
personas accedan al correo
cuando se usa un
computador público o ajeno.

BUENAS PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO INSTITUCIONA



Ingoude Company



REGLA CLAVE: NINGUNA ENTIDAD OFICIAL PIDE CONTRASEÑAS POR CORREO. SI DUDAS, NO HAGAS CLIC Y VERIFICA DIRECTAMENTE EN LA PÁGINA OFICIAL

- Remitente extraño o con errores en el nombre o dominio (ejemplo: soporte@banco-seguro123.com).
- Mensajes urgentes o alarmantes, como “Tu cuenta será bloqueada inmediatamente”.
- Enlaces sospechosos que no coinciden con la página oficial.
- Errores ortográficos o redacción poco profesional.
- Solicitud de datos personales o bancarios, contraseñas o códigos de verificación.
- Archivos adjuntos inesperados.

CÓMO IDENTIFICAR CORREOS FRAUDULENTOS (PHISHING)



Ingoude Company

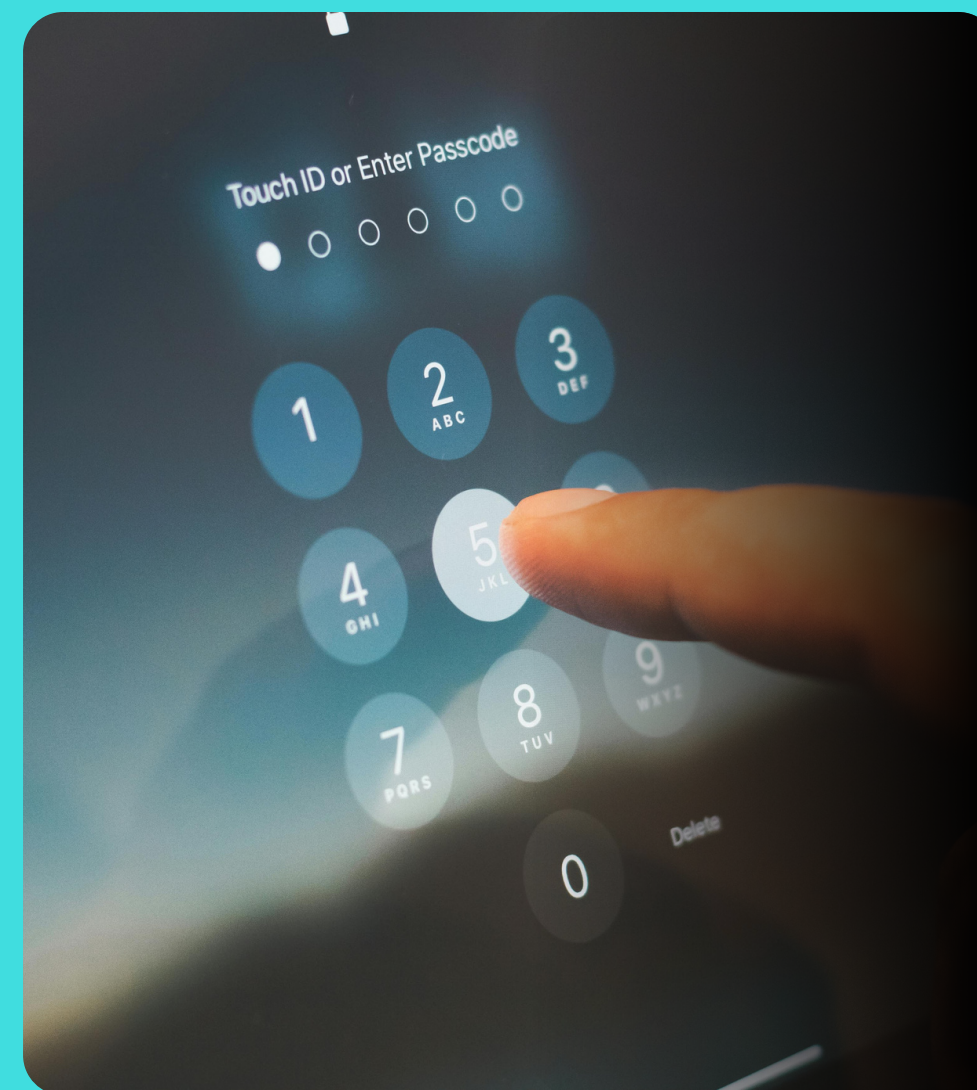


USO SEGURO DE CONTRASEÑAS.

USO SEGURO DE CONTRASEÑAS:

- Crear contraseñas largas y seguras, combinando mayúsculas, minúsculas, números y símbolos.
- No usar datos personales como fechas de nacimiento o nombres.
- No repetir la misma contraseña en diferentes cuentas.
- Activar la verificación en dos pasos cuando esté disponible.
- No compartir contraseñas con otras personas.
- Cerrar sesión en equipos públicos o compartidos.

IMPORTANTE: Una contraseña segura es la primera barrera de protección de tu información.





- Restringir el acceso solo a personas autorizadas mediante contraseñas o permisos.
- Proteger los archivos con clave y evitar compartirlos por medios inseguros.
- Realizar copias de seguridad periódicas para evitar pérdida de información.
- Mantener la información actualizada y organizada, evitando duplicados o errores
- No usar dispositivos públicos para manejar bases de datos institucionales.



MANEJO ADECUADO DE BASES DE DATOS EN EXCEL O SISTEMAS INTERNO

El manejo adecuado de bases de datos en Excel o en sistemas internos implica restringir el acceso únicamente a personal autorizado, utilizando contraseñas seguras y permisos específicos. Es fundamental proteger los archivos con clave, evitar compartir información por medios inseguros y no utilizar equipos públicos para gestionar datos institucionales.

RIESGOS DE COMPARTIR INFORMACIÓN POR WHATSAPP U OTRAS REDES SOCIALES.



Compartir información por WhatsApp u otras redes sociales puede generar varios riesgos, especialmente cuando se trata de datos personales o institucionales. Estos medios no siempre garantizan la seguridad total de la información, lo que puede facilitar la filtración de datos, el robo de identidad o la suplantación. Además, al reenviar mensajes o documentos sin control, la información puede llegar a personas no autorizadas, afectando la privacidad y la confidencialidad. También existe el riesgo de caer en estafas, enlaces maliciosos o archivos con virus.

Por ello, es importante evitar compartir datos sensibles, verificar la identidad de los contactos



Ingoude Company