CIBER SEGURIDAD

CIBERCONSEJOS: SEGURIDAD EN WhatsApp

BICENTENARIO DE BOLIVIA

AGETIC
Digitalizando Bolivia

ESTADO PLURINACIONAL DE BOLIVIA

Consejos para protegerte:

- **No abras enlaces sospechosos** enviados por desconocidos o fuentes dudosas.
- **Habilita la verificación en dos pasos** en la configuración de WhatsApp.
- **Evita descargar archivos o aplicaciones** de fuentes no oficiales.
- **Desconfía de mensajes urgentes** que soliciten datos personales o pagos.
- **Mantén tu aplicación actualizada** para protegerte de vulnerabilidades.

Tu seguridad en WhatsApp depende de ti.
¡Mantente alerta y protege tu privacidad!

5:20 PM

CIBERCONSEJOS

SEGURIDAD EN WHATSAPP

WhatsApp es una de las **aplicaciones de mensajería** más utilizadas en el mundo, pero también es un objetivo frecuente de ciberataques. Conoce los principales riesgos y cómo protegerte.

Principales Amenazas

Malware

» Software malicioso diseñado para recopilar, robar, secuestrar datos, acceder a redes, sistemas, comprometer la privacidad de los usuarios.

AGETIC
Digitalizando Bolivia

Robo de cuenta

» Usan técnicas de engaño para obtener acceso a tu cuenta de whatsapp, se hacen pasar por empresas conocidas.

Phishing

» Técnicas para obtener datos personales mediante mensajes o sitios falsos.

» Suplantan entidades confiables para robar contraseñas o información financiera.

CIBERCONSEJO 1:

MANTÉN ACTUALIZADO TU WHATSAPP

Actualizar WhatsApp no es opcional, es tu defensa diaria.

5:20 PM

AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **Mantener actualizado tu WhatsApp** es fundamental para garantizar la privacidad de tus conversaciones.

» **Cada nueva versión corrige problemas de seguridad** para evitar que ciberdelincuentes espíen tus conversaciones o roben tu información personal.

» **Las actualizaciones incluyen mejoras funcionales** y nuevas medidas de seguridad.

Recomendaciones:

» **Instala la aplicación oficial de WhatsApp** desde fuentes confiables como Google Play Store o App Store.

» **Activa las actualizaciones automáticas** para usar la última versión disponible.

CIBERCONSEJO 2:

NO COMPARTAS EL CÓDIGO DE VERIFICACIÓN

Ignora a quién te pida el código de verificación.

5:20 PM

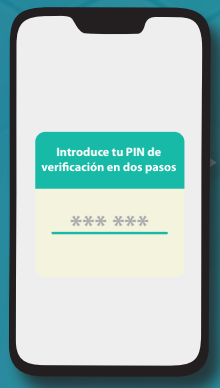
AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **El código de verificación es una clave de seguridad única que se envía a WhatsApp** o por SMS cuando intentas iniciar sesión en un nuevo dispositivo. Este código es esencial para confirmar que eres el propietario legítimo de la cuenta.

» **Si proporcionas el código a alguien más, este podría tomar el control de tu WhatsApp** y hacerse pasar por ti para realizar estafas.

» **Al no compartir el código de verificación estás protegiendo tu cuenta y accesos no autorizados.**



Recomendaciones:

» Si alguien te lo solicita el código de verificación, **ignora el mensaje y bloquea el número.**

» **Nunca compartas tu código de verificación con nadie.**

» **Ni WhatsApp ni ninguna empresa legítima te pedirá este código** por mensaje, llamada o red social.

» **No compartas capturas de pantalla de ese código** bajo ninguna circunstancia.

CIBERCONSEJO 3:

ACTIVA LA VERIFICACIÓN EN DOS PASOS

Añade una capa extra de seguridad a tu cuenta incluso si obtienen tu código de verificación.

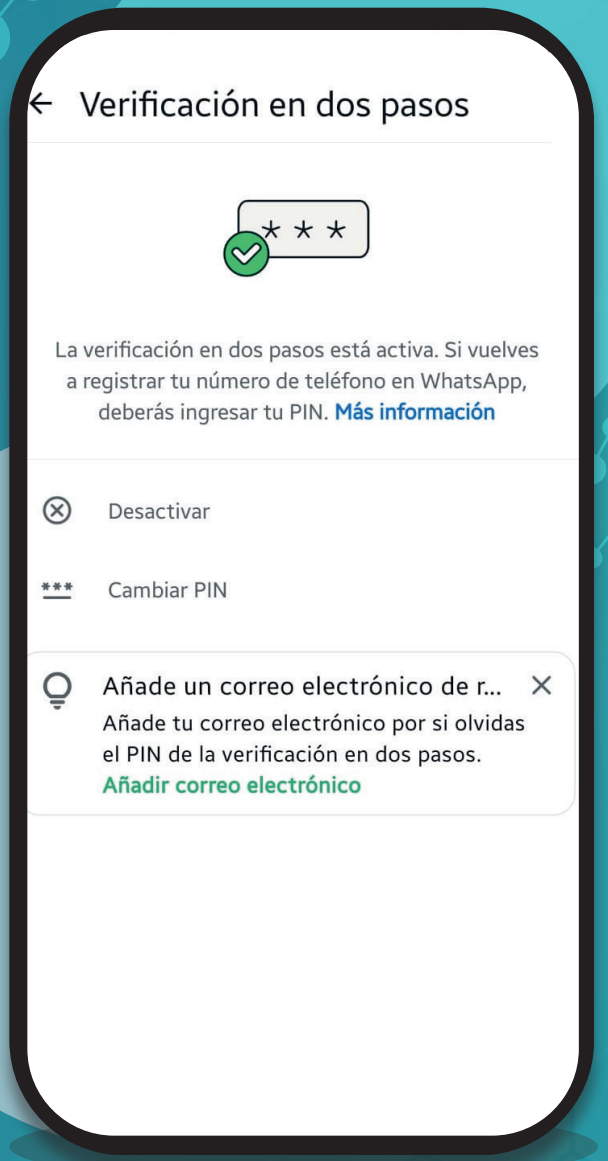
5:20 PM

AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **La verificación en dos pasos** añade una capa extra de protección que impide el acceso no autorizado.

» **Si un atacante obtiene tu código de verificación,** no podrá acceder a tu cuenta sin el PIN de seguridad que solo tú conoces.



CIBERCONSEJOS

AGETIC
Digitalizando Bolivia

ACTIVA CUANTO ANTES LA VERIFICACIÓN EN DOS PASOS PARA REFORZAR LA SEGURIDAD DE TU CUENTA

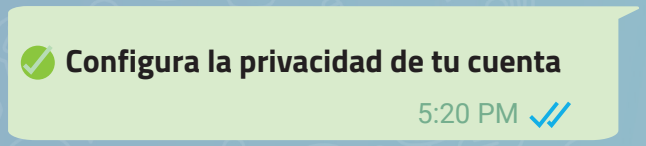
1. Selecciona **Cuenta** > **Verificación** en dos pasos.
2. Pulsa **Activar**.
3. Crea un **PIN de 6 dígitos** personal.
4. Añade **tu correo electrónico** para recuperación en caso de olvido.

EL PIN ES TU LLAVE DE SEGURIDAD, NO LA OLVIDES NI LA COMPARTAS CON NADIE

1. **WhatsApp te solicitará** periódicamente el **PIN** para que no la olvides.
2. **Si olvidaste el PIN**, podrás recuperarlo después de 7 días desde la última verificación.

CIBERCONSEJO 4:

PROTEGE TU PRIVACIDAD



AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» Si no configuras adecuadamente tu privacidad en WhatsApp, **desconocidos podrían ver tu foto de perfil**, tu estado o tu última conexión.

» **Esta exposición facilita la creación de perfiles falsos** que pueden usarse para engañar a otras personas en tu nombre.

» **También incrementa el riesgo de recibir mensajes no deseados,** ser añadido a grupos sin tu consentimiento, ser víctima de acoso digital

Recomendaciones:

» **Revisa y ajusta tus opciones de privacidad** desde la configuración de WhatsApp.

1.Abre**WhatsApp**>**Configuración/ Ajustes / Privacidad**.

2. Configura quién puede ver:

- ✓ **Tu foto de perfil**
- ✓ **Tu última vez y en línea**
- ✓ **Tu información y estado**
- ✓ **Confirmaciones de lectura (puedes desactivarlas si es necesario).**
- ✓ **En Grupos, selecciona “Mis contactos” o “Mis contactos excepto...” para evitar ser añadido sin tu permiso.**
- ✓ **Activa la opción Bloquear contactos si recibes mensajes no deseados.**

CIBERCONSEJO 5:

REVISA PERIÓDICAMENTE LOS DISPOSITIVOS VINCULADOS A TU CUENTA

Asegúrate que solo tu tienes acceso a tu cuenta

5:20 PM

¿Por qué es importante?

» **WhatsApp te permite vincular tu cuenta en otros dispositivos** mediante WhatsApp Web o su versión de escritorio, si pierdes el control de las sesiones activas, podrías estar exponiendo tus conversaciones.

» **Un atacante podría mantener una sesión activa sin que lo notes,** lo que le permitiría acceder a tus mensajes privados, archivos, fotos y contactos sin tu consentimiento.

» **El atacante podría suplantar tu identidad,** extorsionarte o cometer fraudes utilizando tu cuenta, enviando mensajes fraudulentos a tus contactos.

AGETIC
Digitalizando Bolivia

Recomendaciones:

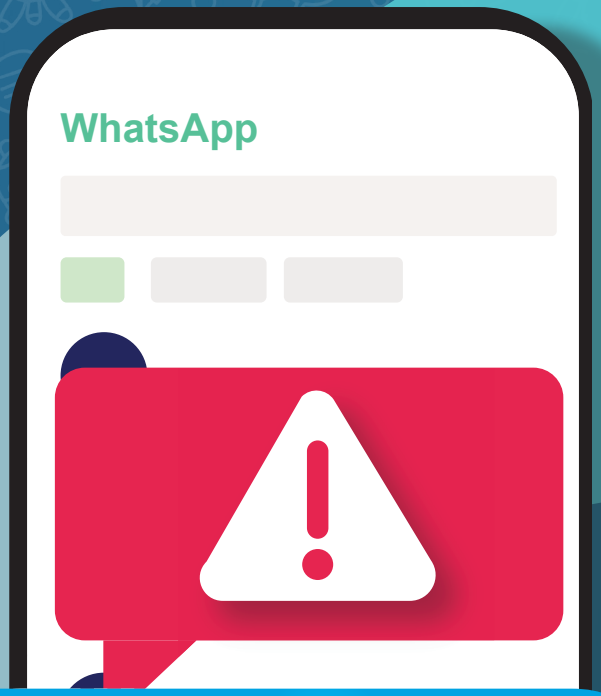
1. Abre WhatsApp y ve a **Configuración** > **Dispositivos vinculados**.

2. **Revisa frecuentemente los dispositivos** conectados desde la configuración de WhatsApp.

3. **Puedes prevenir accesos maliciosos** y proteger tu reputación.

4. Si hay un dispositivo que no reconoces, seleccionalo y **Cierra sesión**.

5. **No dejes tu celular desbloqueado:** cualquier persona podría vincularlo en segundos.



CIBERCONSEJO 6:

NO ABRIR CONTENIDO SOSPECHOSO

Lo desconocido y sospechoso no se abre.

5:20 PM

AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **Al abrir archivos y enlaces sospechosos** podrías infectar tu dispositivo con código malicioso.

» **También podrían robar tus credenciales a través de páginas falsas** que imitan sitios legítimos, llevándote a entregar datos sensibles sin darte cuenta.

» **Además, pueden utilizar enlaces o códigos QR falsos** para realizar estafas económicas, simulando plataformas de pago o promociones engañosas.

Recomendaciones:

» **Evita abrir o compartir enlaces,** archivos o códigos QR que provengan de contactos desconocidos.

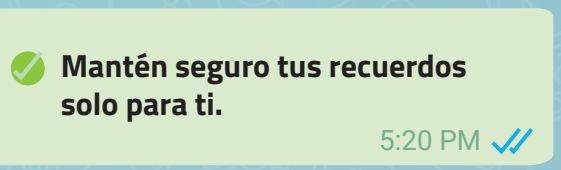
» **Ignora mensajes alarmantes,** urgentes o demasiado buenos para ser verdad, usa el sentido común.

» **Instala y mantén actualizada** una solución antivirus en tu dispositivo.

» **No respondas a mensajes sospechosos,** usa las funciones nativas de WhatsApp para bloquear y reportar.

CIBERCONSEJO 7:

CIFRA TU COPIA DE SEGURIDAD



AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **La copia de seguridad se guarda por separado de la fuente original** para poder recuperar tus conversaciones, fotos y documentos en caso de pérdida del dispositivo.

» **Cifrar tu copia de seguridad es esencial para proteger tus mensajes,** archivos y datos personales, incluso si alguien logra acceder a ella.

» **Sin esta capa de seguridad,** un ciberdelincuente podría acceder a tus conversaciones privadas, fotos, videos o documentos almacenados.

Recomendaciones:

» **Activa el cifrado de extremo a extremo** para la copia de seguridad.

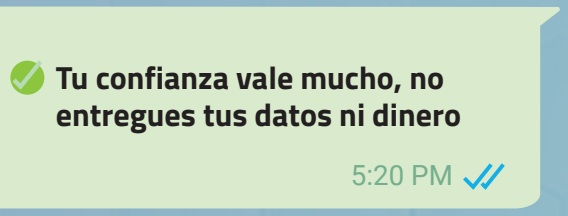
» **Esta función añade una barrera de protección** sobre tu información guardada en la nube.

» **Asegúrate de crear una contraseña segura** o guardar la clave criptográfica en un gestor de contraseñas confiable.

1. Abre WhatsApp > Configuración (Android) / Ajustes (iOS).
2. Ingresa a Chats > Copia de seguridad.
3. Pulsa en Cifrado de extremo a extremo.
4. Selecciona Activar y crea una contraseña
5. Confirma la configuración y guarda la clave de forma segura (no se puede recuperar si la olvidas).

CIBERCONSEJO 8:

PROTEGE TUS DATOS PERSONALES



AGETIC
Digitalizando Bolivia

¿Por qué es importante?

» **Los ciberdelincuentes suelen suplantar la identidad** de familiares, amigos o contactos de confianza para engañarte y obtener información personal o dinero.

» **Las técnicas de ciberestafas** buscan generar urgencia o confusión emocional para que actúes sin verificar.

» **Si no confirmas la identidad del remitente,** podrías enviar dinero a cuentas falsas, compartir datos personales o poner en riesgo a tus contactos si el atacante se hace pasar por ti.

Recomendaciones:

» **Verifica la identidad de la persona,** llama o realiza una videollamada con la persona que supuestamente te escribió.

» **Observa errores ortográficos,** mensajes fuera de contexto o solicitudes inusuales.

» **Desconfía de mensajes** con tono de urgencia o amenazas.

» **No brindes información personal** que pueda usarse para suplantarte.

» **Reporta a WhatsApp y la ATT** el número si confirmas que se trata de un intento de estafa.

AGETIC

Digitalizando Bolivia

Agetic Bolivia

(+591) 63124081

(+591) 63124081