BOLETÍN QUINCENAL DE CIBERSEGURIDAD

# Verificar. Actualizar. Controlar accesos.

Proteger tu empresa comienza con decisiones informadas.

**EDICIÓN 02 / 30 OCTUBRE 2026**

Periodo informativo: 15 al 29 de octubre de 2026


01 / México: suplantación y controles de pago

02 / Servidores y soporte remoto: actualizaciones

03 / Dispositivos móviles: protección y privacidad


---

Noticias, impacto empresarial y acciones prácticas.


**EDICIÓN 02 · INFORMACIÓN PARA DECIDIR**

www.asiscloud.net

## 01 México: verificar antes de transferir

18 de octubre de 2026

La Secretaría de Seguridad y Protección Ciudadana publicó recomendaciones ante la suplantación de directivos y socios comerciales para obtener transferencias o información confidencial. El aviso señala el posible uso de voces e imágenes generadas con inteligencia artificial. Es un comunicado preventivo, no el anuncio de una brecha específica.

**Impacto empresarial.** Una solicitud que parece provenir de un jefe o proveedor puede aprovechar la urgencia para saltarse los controles de pago.

**Qué hacer.** Confirma cualquier cambio de cuenta bancaria por un canal independiente, usando el teléfono previamente registrado del proveedor, y exige doble autorización.

SSPC · Suplantación de directivos y socios comerciales

## 02 PHP: revisar los servidores web

21 de octubre de 2026

ENISA y otras autoridades europeas alertaron sobre CVE-2026-109618 y CVE-2026-109619. Estas vulnerabilidades podrían permitir la ejecución remota de código sin autenticación en servidores afectados. El equipo de PHP publicó actualizaciones ese mismo día.

**Impacto empresarial.** Los sitios, aplicaciones y productos que utilizan PHP pueden necesitar correcciones, incluso cuando ese componente no es visible para el usuario.

**Qué hacer.** Solicita al responsable del alojamiento que confirme si utiliza una versión afectada y documente la actualización. Prioriza los servicios expuestos a internet. El aviso no demuestra que un sitio concreto haya sido comprometido.

ENISA · Comunicado conjunto sobre PHP

## 03 Soporte remoto: corregir BeyondTrust

15 de octubre de 2026 · ampliación del 16 de octubre

BeyondTrust divulgó el aviso BT26-05, correspondiente a CVE-2026-102764, que afecta a Remote Support. El fabricante informó de explotación previa en dos clientes. Los hechos identificados ocurrieron en agosto; la divulgación pública corresponde a esta quincena.

**Impacto empresarial.** Las plataformas de asistencia remota necesitan el mismo control de actualizaciones que los servidores y equipos que administran.

**Qué hacer.** Si utilizas este producto, verifica el parche. El fabricante indica que sus instancias SaaS ya fueron corregidas; las instalaciones propias deben comprobar BT26-05 y seguir las instrucciones para su versión.

BeyondTrust · Aviso de seguridad BT26-05

## 04 iPhone y iPad: también son parte del negocio

26 de octubre de 2026

Apple publicó iOS 27.2 y iPadOS 27.2 con correcciones de seguridad. Su documentación describe, entre otros problemas, accesos indebidos a información sensible y fallas que permitían eludir controles de privacidad.

**Impacto empresarial.** Los teléfonos y tabletas utilizados para correo, documentos y autorizaciones también deben formar parte del mantenimiento de seguridad.

**Qué hacer.** Revisa las actualizaciones oficiales disponibles para cada dispositivo compatible y programa su instalación. En equipos administrados, coordina el cambio con el responsable de TI.

Apple · Seguridad de iOS 27.2 y iPadOS 27.2

# La IA también exige verificar

Una voz o imagen convincente puede formar parte de un engaño. Reconocer a alguien en una llamada no basta para autorizar una operación excepcional. Conserva los procedimientos de validación aunque la solicitud llegue por audio o videollamada: la urgencia no debe sustituir la comprobación de identidad.

Contexto: aviso de la SSPC del 18 de octubre

# Acción práctica de la quincena

## Revisa el correo que controla tu negocio

**01 / Activa la autenticación multifactor.** Comprueba que esté habilitada en el correo principal del negocio.

**02 / Usa una contraseña única.** Evita reutilizarla en otros servicios o compartirla entre personas.

**03 / Revisa cómo recuperar la cuenta.** Confirma que los métodos de recuperación estén vigentes y bajo control autorizado.

**04 / Autoriza solo lo que iniciaste.** Rechaza solicitudes de acceso inesperadas y nunca compartas códigos de verificación.

Medidas permanentes, reforzadas por el aviso de la SSPC del 24 de octubre; no son nuevas funciones ni garantías de protección absoluta.

Fuente: SSPC · Seguridad en cuentas y dispositivos

## Conoce el estado de tu tecnología

**Primera visita diagnóstica sin costo y sin compromiso.**

Auditoría Tecnológica Integral · Blindaje de Información · Servidor Privado de Archivos

Solicitar diagnóstico en asiscloud.net

Los servicios se cotizan posteriormente, según las necesidades identificadas.

Diseño y contenidos desarrollados con apoyo de inteligencia artificial.