01 / EL VALOR DEL MANTENIMIENTO

Mantenimiento de sistemas IP
Revisar, comprobar y documentar.

Guía de revisión de configuración y operación para CCTV y control de acceso. Alcance y pruebas a acordar en cada instalación.

01

Usuarios y permisos

Los permisos excesivos amplían lo que una cuenta puede modificar. [1, 2]

Revisá: cuentas vigentes, accesos compartidos y roles de operación.

Dejá evidencia: usuarios y permisos revisados; bajas autorizadas.

02

Accesos y red

La exposición a Internet y una red sin restricciones facilitan accesos no previstos. [1, 2]

Revisá: servicios publicados, reglas de acceso y separación de redes.

Dejá evidencia: cambios aplicados y acceso autorizado probado.

03

Firmware y soporte

El firmware puede incorporar correcciones de seguridad y errores. Cada modelo tiene su ruta de actualización. [1, 2]

Revisá: modelo completo, versión, soporte y compatibilidad con el sistema.

Dejá evidencia: versión inicial, decisión técnica y versión final.

04

Hora y registros

Una hora coherente permite relacionar eventos; también interviene en la validación de certificados. [2]

Revisá: fecha, zona horaria, sincronización y registros disponibles.

Dejá evidencia: hora verificada y eventos de prueba identificables.

02 / CRITERIOS PARA DECIDIR

Revisar también es decidir.

Matriz de trabajo propuesta por Dialer Medios. Antes de intervenir, contrastá cada hallazgo con documentación del fabricante y con el responsable del sistema.

01 Actualización validada

Si la versión corresponde al modelo y variante, la ruta está documentada y las integraciones fueron validadas: programá la intervención, respaldo y pruebas.

02 Compatibilidad pendiente

Si no están confirmadas las dependencias con grabador, software o integraciones: consultá a soporte y fijá una fecha de resolución. Mientras tanto, evaluá restricciones de acceso con el responsable de red.

03 Equipo sin soporte

Si el fabricante confirma el fin del soporte de seguridad: documentá la situación y proponé un plan de reemplazo. Las restricciones de red pueden reducir exposición, pero no recuperan el soporte del equipo.

04 Cuenta o servicio sin uso confirmado

Antes de quitarlo, identificá su responsable y dependencias. Retirá o restringí solo con autorización; después comprobá que la operación y las integraciones sigan funcionando.

Prioridad: si existe un aviso oficial aplicable al equipo, seguí sus medidas y plazos. Una postergación debe dejar motivo, medida temporal, responsable y fecha de revisión.

03 / INTERVENIR Y COMPROBAR

Una actualización termina cuando el sistema se probó.

Protocolo de trabajo propuesto por Dialer Medios. Ajustalo al modelo, al proyecto y a las funciones contratadas.

01

Prepará la intervención

Registrá modelos y versiones. Consultá documentación oficial, compatibilidades y dependencias. Respaldá la configuración cuando el equipo lo permita.

02

Aplicá cambios controlados

Acordá la ventana de trabajo y el procedimiento de recuperación. Coordiná los cambios de red con su responsable y registrá qué modificaste.

03

Probá las funciones del proyecto

En CCTV: imagen en vivo, grabación nueva, reproducción, exportación y eventos. En acceso: credenciales, permisos y eventos de puerta. Incluí el acceso remoto autorizado.

Protección temporal en la red

El parcheo virtual usa reglas en un firewall o IPS (sistema de prevención de intrusiones) para bloquear patrones de ataque específicos sin modificar el firmware. [3]

No se activa en cualquier cámara o router. Requiere tráfico atravesando el control y protección validada; puede exigir equipamiento, licencias y un especialista de red. No reemplaza la corrección del firmware.

04 / ALCANCE, EVIDENCIA Y ENTREGA

Mantenimiento con evidencia.

El cliente recibe un diagnóstico, acciones verificadas y un plan de pendientes. Ese alcance concreto respalda el valor de tu trabajo.

Definí el servicio por escrito

Equipos y sedes incluidos; tareas y pruebas; modalidad remota o presencial; frecuencia según criticidad y exposición; atención de incidentes, plazos y exclusiones. Cotizá aparte las adecuaciones no incluidas.

Ejemplo ilustrativo de registro

Hallazgo: cuenta de un proveedor anterior todavía habilitada.
Acción: confirmación de que ya no se utiliza y baja autorizada.
Prueba: rechazo del acceso retirado y operación habitual comprobada.
Cierre: fecha, equipo, técnico y autorización referenciada. Registrar resultados sin incluir contraseñas en el informe.

Visita periódica y monitoreo continuo son servicios distintos.
El informe refleja las verificaciones realizadas en esa intervención. El monitoreo continuo, las alertas y la respuesta a incidentes requieren alcance y contratación específicos.

BASE TÉCNICA Y ALCANCE

[1] CISA / NSA · Diez configuraciones deficientes frecuentes (2023).

[2] AXIS OS · Guía oficial de fortalecimiento de seguridad.

[3] Axis · Qué es el parcheo virtual (21/10/2026).

Las fuentes respaldan principios de configuración; los criterios y el protocolo son propuestas de Dialer Medios, no una certificación ni una auditoría integral de ciberseguridad. Funciones sujetas a modelo y firmware. Las referencias extranjeras no crean por sí mismas obligaciones en Argentina. Edición 2 · 23/10/2026.