Estándar para Terceros sobre Sistemas de Televisión por Circuito Cerrado: Buenas prácticas

Versión 1

Fecha: 29/07/2016,

Área de Seguridad de BT

Contenido

1. Introducción

1.1. General

Este documento orienta en las buenas prácticas generales para el uso de la televisión por circuito cerrado (CCTV) por parte de otros proveedores.

1.2. Antecedentes

El uso de CCTV se ha generalizado en todo el Reino Unido en los últimos años. Originalmente instalados para la protección de grandes establecimientos y el monitoreo de centros de ciudades, los sistemas de CCTV se instalan ahora en oficinas, tiendas, escuelas y hasta en vehículos de la red de transporte público. Por otro lado, el mercado ha sufrido una rápida transición de tecnología de grabación análoga a digital, lo cual viene teniendo un impacto significativo en el diseño o las funcionalidades de los sistemas de CCTV.

El foco del documento sigue siendo el mismo: brindar orientación clara a usuarios no técnicos que desean comprar un sistema de CCTV que sirva a todo propósito. Sin embargo, los problemas están en la calidad de la imagen grabada y el archivo de datos, que son componentes esenciales de un sistema digital de CCTV, pero que con frecuencia no se tienen en cuenta a la hora de redactar especificaciones.

Los sistemas análogos de grabación por CCTV eran de diseño relativamente simple, ya que se sustentaban en el uso de cintas de VHS para capturar las imágenes. A diferencia de ellos, los sistemas de grabación digital son mucho más complejos. Graban en una unidad de disco, que solo puede almacenar una cantidad limitada de video; cuando se llena la unidad, el material más antiguo se sobrescribe con el nuevo. Por lo tanto, a la hora de establecer las especificaciones un sistema, se debe considerar la capacidad de la unidad de disco, la provisión de un método adecuado para crear un registro permanente de incidentes clave (por ejemplo, escritor de DVD) y el uso de compresión (que afectará la calidad de imagen grabada). Muchos de estos problemas están interrelacionados; por lo tanto, la mejora en la calidad de la imagen grabada y la mayor frecuencia de cuadro podrían existir a expensas de un menor tiempo de estancia en el sistema. Uno de los objetivos de este documento es proporcionar orientación sobre estos factores complejos.

1.3. Otros materiales y consejos

UK HMG cuenta con una hoja de consejos de alto nivel para la provisión de sistemas de CCTV:

Manual de requerimientos operativos de CCTV	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

El Centro de Protección de la Infraestructura Nacional (CPNI) también brinda orientación sobre protección informática, e incluye secciones sobre el uso de CCTV, tales como:

Televisión por circuito cerrado (CCTV)	http://www.cpni.gov.uk/advice/Physical-security/CCTV/

La Oficina de Comisionados de la Información (ICO) proporciona un código de prácticas de CCTV:

En la imagen: Un código de prácticas de protección de los datos para cámaras de vigilancia e información personal	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

BSI Group también tiene un código de prácticas que está a la venta:

BS 7958:2009 Código de prácticas de operación y gestión de CCTV	http://shop.bsigroup.com/Browse-By-Subject/Security/Electronic-Security-Systems/cctvstandards/

Requerimientos de Seguridad para Proveedores de BT:

Requerimientos de Seguridad para Proveedores de BT V1.1	http://www.selling2bt.com/working/BTSupplierSecurityRequirements/index.htm

La Autoridad de Seguridad en la Industria (SIA) tiene información sobre los requerimientos de licencia de operación de CCTV en espacios públicos:

Vigilancia por CCTV de espacios públicos	http://www.sia.homeoffice.gov.uk/Pages/licensing-cctv.aspx

2. Objetivos

2.1. Este documento busca proporcionar consejos generales sobre seguridad para orientarlo a usted como proveedor de BT con buenas prácticas en el uso de sistemas de CCTV en sus instalaciones, y hace referencia a fuentes de información útil que pueden asistirlo.
2.2. Como proveedor de BT, estará contractualmente obligado a asegurar que toda la información de BT o de los clientes de BT que se le entregue para su cuidado tenga la protección adecuada para garantizar que se cumple con las obligaciones de confidencialidad y seguridad. Deben cumplir con ellas y debe consultar los términos de su contrato y los Requerimientos de Seguridad para Proveedores de BT (ver sección 1.3).
2.3. El sistema de CCTV debe ser solo un componente de su estrategia de seguridad; no debe usarse con exclusividad. No reemplaza al personal de seguridad, aunque pueda permitir que la cantidad de personas necesarias sea menor o que se los reubique en otras actividades de seguridad.
2.4. En su forma más simple, un sistema de CCTV consta de una cámara de televisión conectada por medio de un enlace de transmisión, que puede ser un cable, a un monitor ubicado en la sala de guardias o en el centro de control. Otros sistemas más complejos utilizan varios monitores y cámaras o un único monitor con un sistema de cambio de imagen que muestra cuadros de la cámara en secuencia. Se pueden agregar otros elementos, como grabadoras o sistema de cambio de imagen automático en respuesta a una señal de alarma.
2.5. Los sistemas de CCTV permiten aclarar si un alerta de seguridad es real y son vitales para las investigaciones posteriores a incidentes, pero solo si la calidad de las imágenes es buena y permite que se identifique qué sucedió y que puedan usarlas las autoridades, o bien le lleva tranquilidad a usted, a BT o a terceros de que los incidentes se están tratando adecuadamente.
2.6. La iluminación externa ayuda al personal de seguridad y mejora las capacidades de los sistemas de CCTV si se diseña y se utiliza con criterio. Los sistemas eficaces de CCTV ayudan a disuadir un incidente o incluso a identificar actividades de planificación. Las imágenes de buena calidad pueden brindar pruebas clave en el curso de una investigación y asistencia a la autoridades. También puede utilizarse como alarma si viene asociada a un método de ‘detección de movimiento’.
2.7. Si ha contratado personal interno que opere el equipo de CCTV, debe asegurarse de que tengan las licencias correspondientes de la Autoridad de Seguridad de la Industria (SIA) y de que esas licencias siguen estando vigentes mientras operan el equipo de CCTV para usted. Es delito no tener las licencias. Eso cobra especial importancia si el equipo de CCTV está instalado en posiciones fijas o tiene capacidades de paneo, inclinación y zoom; y cuando los operadores monitoreen en forma proactiva las actividades del público ya sea en lugares públicos o en propiedad privada, usen cámaras para enfocarse en las actividades de ciertas personas en particular ya sea controlando o dirigiendo las cámaras hacia las actividades de individuos, usen las cámaras para buscar individuos específicos, usen imágenes de CCTV grabadas para identificar individuos o para investigar sus actividades.
2.8. La utilización y el fin de un sistema de CCTV deben estar registrados en su política de seguridad, la cual debe estar documentada y guardada para demostrar cumplimiento regulatorio. El Apéndice A contiene una lista de temas sugeridos para esta política.

3. Calidad de las imágenes grabadas

3.1. Antes de instalar un sistema de CCTV, deberá tener una idea clara de lo que espera que haga el sistema y de cómo debería rendir. Eso incluye qué quiere ver y dónde exactamente: por ejemplo, reconocer la cara de alguien que cruza una puerta, leer el

número de placa de un vehículo o grabar un tipo de actividad en particular, como puede ser caminar por una sala, cambiar moneda o un ataque.

3.2. Tanto la resolución como el nivel de compresión y la cantidad de imágenes por segundo vendrán determinadas por lo que usted desee ver en la grabación. Si no puede verlo es porque no se ajusta a lo que busca. No espere tener mayor nivel de detalle con funciones de mejora como los controles de zoom.

3.3. Una buena manera de asegurar que el sistema es capaz de atender las necesidades es una hacer una prueba subjetiva. Instale una cámara y pídale a alguien que cruce la puerta o estacione el automóvil en el lugar de interés y grabe las imágenes. Debe hacerlo en las condiciones en que supuestamente operaría el sistema; es posible que el rendimiento del equipo sea distinto cuando hay varias cámaras grabando.

3.4. La calidad de los imágenes grabadas o impresas podría diferir de lo que ve en vivo. No debe comprometerse la calidad de las imágenes para grabar más en el sistema. Existe un alcance para el uso de una escala proporcional de calidad de imagen según el momento en que se graba. Por ejemplo, el video de alta calidad y con alta frecuencia de cuadro durante las primeras 24 horas con incremento gradual de la compresión o descenso de la frecuencia de cuadro después de eso, pero manteniendo las imágenes durante al menos 20 días. Eso dependería de la naturaleza de la instalación y del tipo de grabaciones que se están realizando.

3.5. Para garantizar la calidad de grabación continua, es esencial que se realice el mantenimiento regular de todos los aspectos del sistema, en especial enfoque de la cámara, limpieza de los lentes, soportes, etc.

3.6. Se debe también contar con iluminación adecuada perimetral y local (para facilitar la observación natural y para la seguridad del personal), complementada con luces infrarrojas o similares, para así lograr una imagen satisfactoria del sistema de CCTV en todo momento, noche y día, que permita detectar la imagen que aparece en la pantalla como una persona; es decir, una imagen que cubra al menos el 50 % de la altura de la pantalla. En estos casos es que sirve de asistencia para el control de acceso o con fines de ‘reconstrucción de incidentes’.

3.7. El sistema debe poder ser capaz de garbar continuamente, y es mucho mejor si se lo monitorea ‘en vivo’ para responder ante un incidente o detectar signos de intrusión. Es fundamental tener una plan de respuesta implementado.

3.8. Las cámaras deben mantenerse en buen estado operativo (no deben estar fuera de servicio o defectuosas). La hora que muestra la cámara debe ser precisa.

3.9. Se debe firmar un Acuerdo de Nivel de Servicio (SLA) con el tercero proveedor de servicios de mantenimiento que garantice la reparación de las cámaras en forma oportuna.

4. Almacenamiento

4.1. El acceso al sistema y a las imágenes grabadas debe estar controlado para evitar que se manipulen o que las vea alguien sin autorización. Los métodos de protección electrónica que exigen hardware o software comercial entorpecerán una investigación si no permiten que las imágenes puedan compartirse con terceros autorizados. Los métodos físicos de control de acceso, como ser la ubicación del sistema en una sala cerrada con llave, tienen el mismo nivel de efectividad si se los documenta apropiadamente. Eso sucede para garantizar que se mantenga la integridad de imágenes almacenadas.

4.2. A los fines de una investigación, es importante que las grabaciones cubran un periodo extenso. Podría resultar útil retener las imágenes por más de 20 días en ciertas circunstancias, pero esto no debería afectar la calidad de las grabaciones más recientes.

4.3. Debe ser posible proteger imágenes o secuencias específicas, identificadas como pertinentes para una investigación, para evitar que se sobrescriban antes de que las vea o las extraiga un investigador.

4.4. Las obligaciones contractuales de BT especifican que las imágenes deben guardarse 45 días (requerimientos de SBCA) o 20 días (Requerimientos de Seguridad de BT), y eso incluye las imágenes de respaldo. Las imágenes deben guardarse durante un mínimo de 20 días.
4.5. Los proveedores deben extender este periodo en ciertas situaciones, a saber:
4.6. Debe guardarse prueba en video de CCTV para una investigación penal en curso.
4.7. Los estándares de seguridad de la industria, como NACOSS (Consejo Nacional de Aprobación de Sistemas de Seguridad), especifican un periodo de retención definitivo.
4.8. Se especifica como requerimiento necesario en países fuera del Reino Unido para cumplir con la legislación local.
4.9. Una vez que vence el periodo de retención, todas las imágenes de CCTV deben borrarse (es aceptable sobrescribirlas).
4.10. Todas las grabadoras de video digital y video de CCTV deben estar instaladas en lugares discretos para evitar el acceso no autorizado y la posibilidad de que alguien vea el contenido de las pantallas de CCTV.
4.11. Solo el personal autorizado tiene acceso a todas las grabadoras de video digital de CCTV; y el acceso a las imágenes debe estar protegido con contraseña.
4.12. Las imágenes grabadas de CCTV deben tener copia de respaldo, e, idealmente, deberían guardarse en un lugar separado.

5. Exportación de imágenes

5.1. Si sucediera un incidente de seguridad, es importante que el sistema pueda exportar copias del metraje del sistema de CCTV para ayudar en la investigación y a las autoridades. Es poco probable que el investigador sepa cómo operar su sistema. Para facilitar la reproducción y exportación, debería haber en el lugar un operador capacitado y una guía de usuario simple.
5.2. Exportar volúmenes medianos o grandes de datos puede insumir una cantidad sustancial de tiempo. El operador debe conocer cuál es el periodo de retención del sistema y el tiempo aproximado para exportar volúmenes de datos pequeños (por ejemplo, 15 minutos), medianos (por ejemplo, 24 horas) y grandes (hasta todo el sistema).
5.3. Si el software que se necesita para reproducir las imágenes no está incluido en la exportación, es posible que los terceros autorizados no puedan verlas. Exportar la pista de auditoría o el registro de eventos del sistema, y la configuración del sistema junto con las imágenes ayudará a mantener la integridad de las imágenes y el sistema.
5.4. La cantidad de video que necesita exportar un investigador dependerá de la naturaleza de la investigación. Por ejemplo, un robo en una oficina podría requerir solo un par de instantáneas o una secuencia corta. No obstante, un incidente más grave podría exigir que se exporte hasta todo el video contenido en el sistema. Es esencial que el sistema pueda hacerlo rápidamente y a un medio adecuado. Una solución ideal para descargas medianas a grandes es que el sistema cuente con la posibilidad de exportar a una unidad de disco *plug-and play*. Exportación y grabación deben poder ocurrir en simultaneo sin afectar el rendimiento del sistema.
5.5. El sistema no debe comprimir imágenes cuando se exportan del sistema, ya que esto podría reducir la utilidad del contenido. También, la imagen no debe sufrir conversión alguna de su formato que afecte el contenido o su calidad.

6. Reproducción de imágenes grabadas

6.1. El software u otra tecnología utilizada para la reproducción debe permitir la búsqueda eficaz en las imágenes y que se vea toda la información contenida en ellas y asociada con

ellas. La reproducción de los archivos exportados debe poder ser inmediata; por ejemplo, sin reindexación de los archivos ni verificaciones.

7. Ubicación de las cámaras

7.1. Plano del emplazamiento:
La primera tarea a la hora de redactar un requerimiento operativo es dibujar un plano del emplazamiento y marcar en él las áreas de interés. Cuanto mayor sea el detalle del plano, mejor, ya que eso ayudará en la ubicación de las luces y las cámaras, en especial en referencia a los campos visuales y los problemas ambientales potenciales, tales como follaje o sol bajos.

7.2. El próximo paso es determinar los problemas que afectan al emplazamiento. Algunos de ellos pueden ser amenazas generales, pero otros podrían ser específicos de un lugar en particular. Estas son algunas amenazas que podrían identificarse:

- Control de masas
- Robo
- Entradas no autorizadas
- Seguridad pública

7.3. Esos problemas potenciales y/o amenazas pueden marcarse en el plano del emplazamiento. Esto se usa luego para visualizar la escala del problema y el nivel de cobertura que se necesita. Algunas áreas, tales como entradas y salidas, podrían necesitar cobertura para distintas actividades, es decir, monitorear el flujo de personas e identificar personas en casos de robos o similares.

7.4. El sistema de CCTV exterior debe estar colocado de manera tal que cubra el perímetro, el acceso (entrada/salida) al edificio y otras áreas sensibles, tales como el depósito de diésel, paneles de energía, generadores de energía, etc.

7.5. Si hay dispositivos de detección de movimiento, el campo visual de la cámara debe estar enfocado correctamente de manera que no quede tan reducido que no grabe nada.

7.6. Cuando el sistema esté instalado en el interior, deberá ser en un lugar desde el que monitoree que todos los puntos de entrada y salida de todas las áreas de BT y otras sensibles, como ser el Centro de Datos, la sala de Comunicaciones, las áreas de reunión comunes etc. estén cubiertos pero no deberá instalarse donde pudieran capturar información de BT en las pantallas.

8. Evaluación de los riesgos

8.1. A la hora de instalar y usar sistemas de CCTV, los proveedores deben evaluar regularmente los riesgos para la seguridad que pretenden cubrir con el sistema de CCTV. Esas evaluaciones deben contemplar lo siguiente:

¿Cuál es la probabilidad realista de que suceda determinada actividad?

- Baja / Media / Alta

¿Cuáles serían las consecuencias de que esa actividad no se monitoree y/o grabe?

- Menores / Moderadas / Graves
- Por ejemplo, ¿la actividad causará pérdidas económicas o comprometerá la seguridad del personal o del público?
- ¿Puede priorizar las actividades que desea monitorear?

- ¿Podría usar métodos alternativos (o más económicos) para manejar la actividad, como ser mejor iluminación, rejas o alarmas contra intrusos?
- ¿La actividad podría ser un problema de corto o largo plazo?

9. Determinación de la solución más eficaz

9.1. Una vez que las áreas problemáticas y las amenazas potenciales están indicadas en el plano, se puede realizar una evaluación de las soluciones más eficaces. Es probable que el sistema de CCTV sea solo uno de una variedad de opciones y deberá considerarse en el contexto de una auditoría de seguridad más amplia, junto con otras medidas tales como:

- Iluminación
- Barreras o protección física
- Alarmas de proximidad o sistemas de detección de intrusos
- Mejor diseño de emplazamiento o eliminación de amenazas

Por otra parte, existen varias situaciones en las que un sistema de CCTV bien diseñado podría resultar beneficioso. Por lo general, caen en una de tres grandes categorías:

- Seguridad
- Disuasión
- Investigaciones de delitos

10. Criterios de éxito

10.1. A la hora de instalar y utilizar sistemas de CCTV, los proveedores deben evaluar regularmente si el sistema está bien instalado. Esas evaluaciones deben contemplar lo siguiente:

Una vez detectada una actividad, ¿cuál sería un resultado satisfactorio?

- Prevención de robos o daños
- Identificación de intrusos
- Mejora en el flujo de tráfico
- Disuasión de una actividad

El éxito quedará determinado por una combinación del nivel de eficacia con que funciona el sistema y el grado de cumplimiento de los requerimientos operativos.

¿Con qué frecuencia espera que el resultado sea satisfactorio?

(por ejemplo, ¿qué nivel de eficacia o confiabilidad deberá tener la tarea?)

- Todo el tiempo
- En la mayoría de las ocasiones
- Siempre durante el día, pero solo en ocasiones después del horario laboral

Frecuencia de los riesgos e incidentes que no se atienden con un sistema de CCTV.

Control de documentación

Estándar para Terceros sobre Sistemas de Televisión por Circuito Cerrado: Buenas prácticas

Redactado por: Área de Seguridad de BT

Versión 1, publicado el 1.° de agosto de 2016

11. Apéndice A

¿Qué debería incluir una política de seguridad con CCTV?

La siguiente lista no pretende ser exhaustiva ni obligatoria, sino que señala buenas prácticas:

- Detalles sobre el sistema de CCTV;
- Objetivos de la instalación del sistema;
- Declaración de intención;
- Manera en que se utiliza el sistema de CCTV; por ejemplo, si graba continuamente o no, si tiene sensores de movimiento, infrarrojos, etc.
- Operación del sistema;
- ¿Está monitoreado por un Guardia de Seguridad o avisa a un Centro de Gestión de Alarmas?
- Ubicación de las cámaras;
- Lugar de almacenamiento de las imágenes;
- Periodo de retención de las imágenes;
- Personas que puedan acceder a las imágenes;
- Respaldo;
- Detalles de mantenimiento;
- Forma de manejar los incidentes fuera de horario laboral;
- Detalles del proceso instaurado para gestionar las solicitudes para ver las imágenes;
- Detalles de auditorías o controles proactivos regulares para asegurar que se cumplen los procedimientos;
- Roles y responsabilidades; por ejemplo, el rol del operador de CCTV debe definirse en una Descripción de Tareas;
- Fines específicos y bien definidos del uso de la información y detalles de la manera en que se los ha comunicado al personal que opera el sistema;
- Estipulaciones de que el sistema de CCTV debe usarse en cumplimiento con la legislación local.