# CBSF, una solución frente a las nuevas amenazas

**Manuel Carpio**
Asesor Senior de Ciberseguridad de Inerco Security

**Raúl Porras**
Ingeniero de Proyectos de Inerco Security

En artículos anteriores en esta misma revista, titulados "Ciberseguridad de los sistemas de seguridad físicos, un flanco abierto"[1] y "Los centros de control de seguridad en la próxima guerra híbrida"[2], hemos venido comentando cómo los miles de centros de control de seguridad existentes en España se enfrentan a un conjunto nuevo de amenazas.

La existencia de redes ethernet en los sistemas de seguridad (frente a transmisiones puramente analógicas y a través de buses propietarios), la disposición de sistemas operativos estándares sobre los que se soportan las aplicaciones de control de seguridad, la interconexión de estas plataformas informáticas con el exterior para mantenimiento o exportación/importación de datos (de control de accesos, por ejemplo), etc., han permitido el éxito de múltiples amenazas.

Conseguir la desactivación o anulación del servicio completo del centro, la extracción de datos no autorizada (vídeos de incidentes, por ejemplo), el borrado de imágenes de incidentes pasados o la creación de tarjetas de control de accesos no autorizada ya no es ciencia ficción, sino que está pasando en la actualidad en múltiples instalaciones, algunas de las cuales Inerco Security ha auditado o peritado por requerimiento judicial.

## Vulnerabilidad evitable

Las amenazas que aparecen por la conexión con el exterior de los centros de control de seguridad física pueden afrontarse fácilmente. Básicamente, la principal vulnerabilidad y el origen de otras derivadas que explotarán dichas amenazas es, en muchos casos, la no existencia de un administrador específico del sistema informático, que es en realidad un centro de control de seguridad. Por otra parte, por diversas razones históricas, aun existiendo un eficiente departamento de ciberseguridad en las empresas, este no ha incluido entre sus activos a proteger el propio centro de control de seguridad.

Estas circunstancias derivan en que el director de Seguridad, "propietario" del centro de control, no conoce el nivel de "cibervulnerabilidad" que tiene y se fía de la empresa de mantenimiento del sistema de seguridad que le atiende. Se genera una "tierra de nadie" no atendida.

**Las amenazas que aparecen por la conexión con el exterior de los centros de control de seguridad física pueden afrontarse fácilmente**

Evidentemente, lo primero que hay que tener en cuenta para salir de esa situación es conocer el nivel de vulnerabilidad existente (qué frentes están abiertos) y dimensionar y priorizar las acciones a realizar para remediarlo.

## Servicio CBSF

Desde Inerco Security venimos prestando un servicio de Estudio de la Ciberseguridad en Sistemas de Seguridad Físicos, llamado CBSF, que en esencia permite:

- Conocer las vulnerabilidades existentes ante las nuevas amenazas en los centros de control de seguridad.
- Exponer, evaluar y priorizar las soluciones necesarias para contrarrestarlas.

Para ello, el servicio lo dividimos en dos fases: una primera de auditoría, en la que se obtiene una evaluación detallada del estado de ciberseguridad del centro de control de seguridad; y una segunda etapa en la que se especifican las medidas correctoras necesarias para resolver las vulnerabilidades detectadas en la fase anterior.

Fase de Auditoría y Evaluación:

Para llevar a cabo la primera etapa de auditoría y evaluación se emplea un conjunto de controles clave extraídos en base a nuestra experiencia a partir de regulaciones y normativa de referencia, tanto del ámbito físico como del lógico (ISO/IEC 27002:2013, Esquema Nacional de Seguridad, Normativa UNE de Seguridad Física, Ley PIC, etc.).

Desde Inerco Security unimos el conocimiento profundo de ambos sectores integrando equipos de trabajo con gran experiencia en seguridad física y ciberseguridad, lo que hoy en día resulta necesario, ya que los centros de control de seguridad deben diseñarse considerando esta última como un requisito y punto de partida de diseño adicional.

Gracias a esta unión, el conjunto de controles desarrollados permite evaluar las medidas de ciberseguridad consideradas en el centro de control de seguridad y que serían aplicables al *software* y *hardware* específico de los sistemas de seguridad físicos. Además, permitiría evaluar otras características adicionales como son la operación y gestión del sistema de seguridad, la funcionalidad de los sistemas de centralización empleados y las medidas de protección físicas usadas para la protección del centro de control de seguridad y áreas críticas. Por tanto, el conjunto de controles se agrupa en cuatro dimensiones que permiten evaluar:

- Las medidas técnicas de **ciberseguridad** implantadas.
- Las medidas organizativas de la **operación** del sistema de seguridad.
- La **funcionalidad** específica del sistema de seguridad administrado.

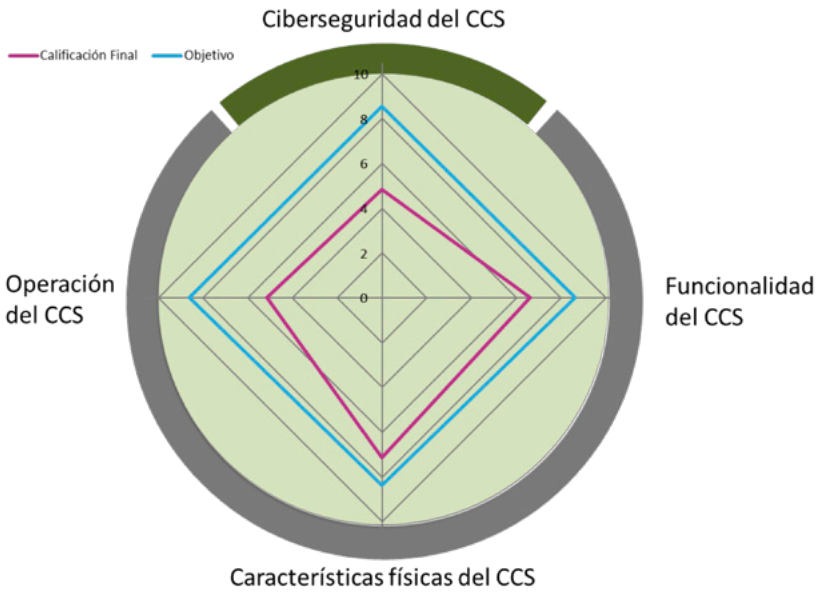


Gráfico 1. Ejemplo de un diagrama de resultado de evaluación.

- Las medidas de **seguridad física** empleadas para la protección del centro de control y salas técnicas dependientes del mismo.

Los controles han sido catalogados con tres niveles de prioridad proporcionándoles pesos característicos en función de la prioridad asignada. Los resultados de la evaluación se presentan en diagramas que permiten intuir fácilmente el estado y situación en cada una de las dimensiones evaluadas, tal y como se puede apreciar en el gráfico 1 de ejemplo.

En cada una de las dimensiones evaluadas, el conjunto de controles se ca-

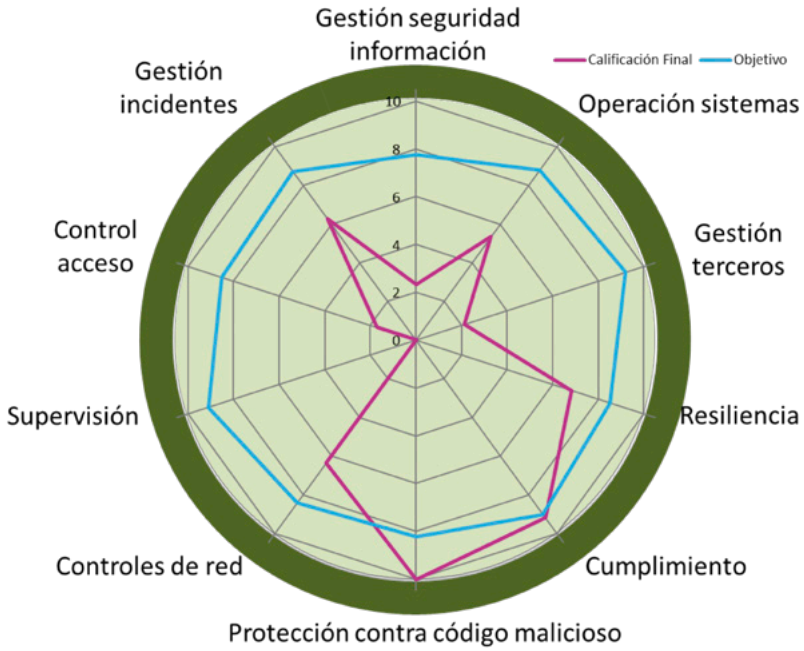


Gráfico 2. Ejemplo de resultado de evaluación de la dimensión de ciberseguridad.

tegoriza a su vez en diferentes secciones que hacen referencia a distintas áreas, actividades y capacidades propias de la dimensión en cuestión que se está evaluando. En la dimensión de ciberseguridad los controles y medidas seleccionadas se categorizan en 14 secciones que permiten cubrir totalmente las distintas áreas consideradas por las regulaciones y normativas de seguridad informática de referencia consideradas (gestión de la seguridad de información, resiliencia, controles de red o cumplimiento, entre otros). Para facilitar la comprensión del resultado obtenido del diagnóstico desarrollado para cada una de las secciones que afectan a la dimensión de ciberseguridad, los resultados se presentan también gráficamente. En el gráfico 2 se puede observar un ejemplo del resultado que se obtendría (el paso de 14 a 10 secciones se debe a que en algunos casos no aplican todas).

Este ejemplo es extrapolable a cada una de las demás dimensiones evaluadas. En la dimensión de funcionalidad del sistema de seguridad administrado se consideran controles específicos para cada uno de los subsistemas de seguridad (detección de intrusión, control de accesos o circuito cerrado de televisión, entre otros), mientras que en la dimensión de operación se tienen en cuenta controles que evalúan, por ejemplo, la gestión de incidentes y operativa de los distintos operadores del centro de control de seguridad. Por último, en la dimensión de medidas de seguridad física se evalúan tanto las medidas de protección empleadas para proteger la instalación del centro de control, como medidas adicionales que consideran la calidad y el diseño ergonómico tenidos en cuenta.

Fase de Especificación de Medidas Correctoras:

En la segunda etapa se especifican las medidas correctoras en base al Plan de Actuación desarrollado en la fase anterior de auditoría. En este plan se establece la priorización, la importancia y el planteamiento a seguir para conseguir un nivel adecuado en cada una de las dimensiones estudiadas.

La especificación de medidas correctoras tiene la finalidad de permitir que el cliente pueda llevar a cabo una fase de petición de ofertas de los suministros y servicios necesarios para dotarse de las medidas correctoras recomendadas, ya sea como petición interna al departamento correspondiente del cliente o a empresas externas correspondientes de cada especialidad. Desde Inerco Security se apoyará en todo momento al cliente en la fase de ejecución e implementación de dichas medidas para que se cumpla con las especificaciones definidas.

Los suministros y servicios especificados que no sean característicos de consultoría podrán ser prestados por empresas especializadas de servicios de ciberseguridad externas o prestarse directamente por servicios internos del propio cliente.

**La principal vulnerabilidad y el origen de otras que explotan las amenazas es, en muchos casos, la no existencia de un administrador del sistema informático**

## Servicios relacionados

Como labor de consultoría adicional que ofrecemos para complementar el servicio del CBSF, proponemos la monitorización continua del sistema mediante la revisión del cumplimiento del plan de trabajo a partir de la realización de auditorías periódicas (anuales o semestrales) que permitan al cliente conocer en todo momento la evolución y mejora del estado de cada una de las dimensiones evaluadas en función de la implantación de las diferentes medidas correctoras especificadas que son llevadas a cabo.

Por otro lado, una vez obtenido un nivel adecuado de ciberseguridad apoyamos y acompañamos al cliente, si así lo requiere, en procesos de certificación de la seguridad implantada en diferentes organismos de certificación nacionales o internacionales.

Adicionalmente, desde Inerco Security ofrecemos otros servicios relacionados como revisiones en *legal compliance* y realización de análisis de riesgos tanto físicos como lógicos.

## Necesidad

Como hemos visto, la aparición de las nuevas amenazas informáticas que afectan directamente a los sistemas que ya no se encuentran aislados y que permiten la operación y gestión de los centros de control de seguridad tiene varias consecuencias.

- Es necesario cambiar la mentalidad actual en cuanto a los requerimientos que han de tenerse en cuenta durante el diseño e implementación de estos centros.
- Se precisa evaluar consecuentemente el estado de la ciberseguridad de los sistemas físicos, los cuales se han convertido en un flanco abierto para los ciberdelincuentes que podrían explotar las distintas vulnerabilidades de estos sistemas y, por tanto, causar incidentes graves en infinidad de instalaciones.

## Referencias

1. Bilbao, E. (octubre, 2018): "Ciberseguridad de los sistemas de seguridad físicos: un flanco abierto". *Seguritecnia*, nº 457 (p 64-66).
2. Carpio, M. (febrero, 2019): "Los centros de control de seguridad en la próxima guerra híbrida". *Seguritecnia*, nº 461 (p 50-51).