

# Cerberero

## Lector de Triple Tecnología

Convergencia entre la Seguridad Física  
y Lógica en Instalaciones Críticas



**Firma Digital**



**Huella Dactilar**



**Código Alfanumérico**

## Antecedentes

Las condiciones de mercado y el entorno global exigen a los responsables de seguridad manejar plataformas inteligentes donde se pueda gestionar con eficacia y eficiencia los riesgos inherentes a los procesos críticos.

En el modelo tradicional de seguridad, el concepto de seguridad se basa en un escenario local donde se pretende la protección de las personas, los valores y la infraestructura. Esta percepción en el nuevo modelo integral abarca, además de los anteriores, la protección de la información o el conocimiento y los procesos, productos y servicios inherentes a la compañía, además, el ámbito de protección migra hasta un ámbito global desde el local mencionado anteriormente.



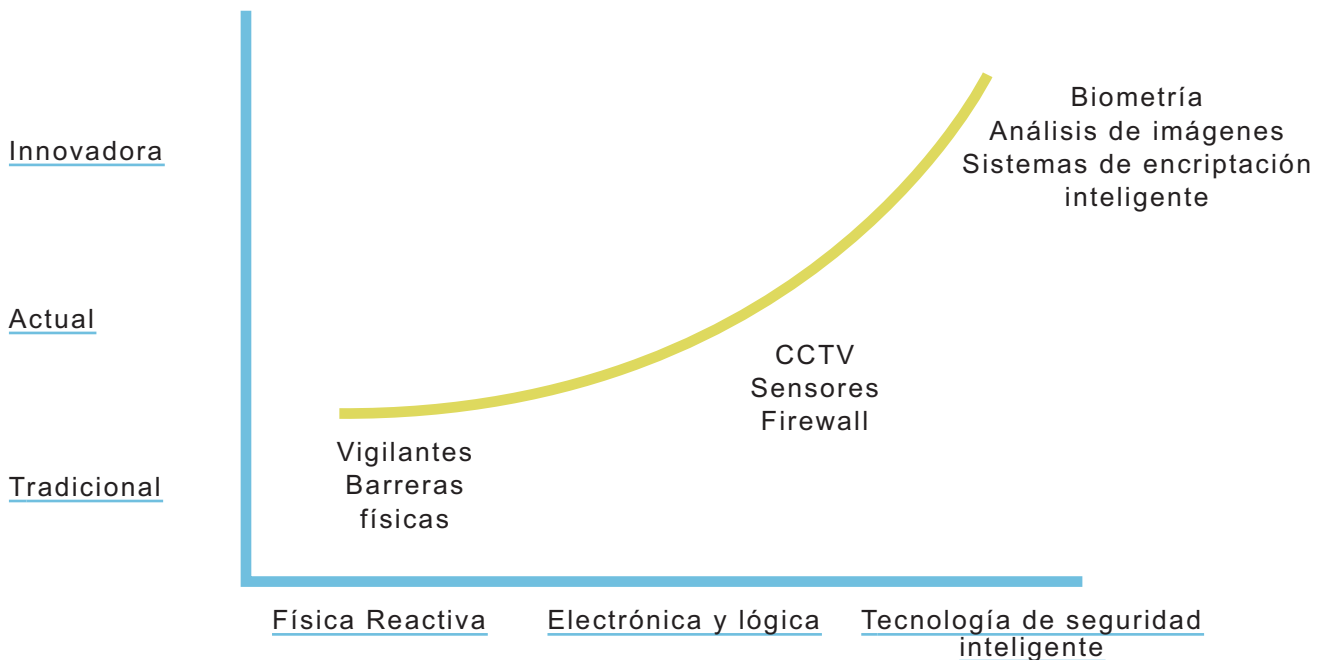
Pero es fundamental que a nivel descriptivo entendamos qué abarcan los conceptos de seguridad física y seguridad lógica. El objetivo de las soluciones de **seguridad física** es resguardar la seguridad patrimonial de las personas, comunidades y organizaciones. Por el contrario, la **seguridad lógica** se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información que podemos encontrar en todo diseño de seguridad de por ejemplo un CPD. La seguridad lógica involucra todas aquellas medidas establecidas para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

## Evolución

La evolución de los sistemas de seguridad es pareja a la evolución de los métodos delictivos que se usan. En los años setenta los principales riesgos existentes eran los robos y asaltos, la política de seguridad era una política de seguridad física reactiva por medio principalmente de medios de vigilancia (normalmente humana) y barreras físicas.

Desde los años noventa, se produjo la primera evolución significativa incluyéndose de modo relevante en los índices de impacto delictivo la estafa, las falsificaciones, el fraude y el lavado de activos. En esta fase, es cuando se consolidan y establecen los conceptos de seguridad electrónica como parte de los medios de seguridad física establecidos hasta ese momento y el concepto de la seguridad lógica. A partir de esta etapa los medios de protección principalmente usados son los sistemas de videovigilancia y sensores en las áreas de seguridad electrónica y los firewall en las de seguridad lógica.

Pero en un mercado globalizado a todos los niveles, se exige un nuevo paso evolutivo. Las últimas tendencias de seguridad dotan a los sistemas de seguridad física de métodos predictivos, **criptográficos** o analíticos en base a información adquirida a través de mediciones biométricas o análisis de imagen, **certificados digitales**.



**Convergencia: nueva tendencia de seguridad.**

Hasta estos momentos los mundos de la seguridad electrónica y la seguridad lógica han trabajado en paralelo cruzándose e incluso chocando en algunos aspectos de sus conceptos de implantación o diseño.

Cuando ACAL BFI IBERIA inició el desarrollo del lector de triple tecnología Cerbero para gestionar en un único dispositivo electrónico la seguridad física y lógica de un recinto (por ejemplo un CPD), el principal reto planteado era el diseño de un terminal de control de accesos de absoluta fiabilidad. Por una parte, debía implementar las tecnologías de identificación más avanzadas de ambos sectores (biometría, criptografía, contraseña alfanumérica y firma digital) y todo el proceso de Alta/Bajas de usuarios desde una única estructura jerárquica mediante la coordinación con el servicio de "Directorio Activo".

Tras el estudio inicial de necesidades, se estableció el documento de definición técnica de las prestaciones a implementar y a partir del cual se realizó el primer prototipo. Desde entonces hasta ahora el lector de triple tecnología Cerbero, ha crecido bajo el objetivo de disminuir y optimizar su operación en la identificación y verificación del usuario. El estado actual del arte Cerbero se encuentra en su tercera generación, su flexibilidad es tan formidable que le permite adaptarse a diversos y variados requerimientos operativos e incluso interactuar en la verificación con otros sistemas (local/remotamente) para incrementar de forma significativa el nivel de seguridad en instalaciones críticas como los CPDs.

**Cerbero** es un sistema de control de accesos orientado a fusionar y aprovechar las sinergias de las implementaciones a nivel corporativo de ambos criterios de seguridad.

**Cerbero** es un terminal de accesos de triple tecnología que permite realizar la verificación de acceso a un área restringida;

1 Mediante identificación biométrica de huella dactilar,

2 Acceso a la tarjeta contenedora de los certificados, mediante password.

3 Tras el acceso al contenido público de la tarjeta, se realiza la comprobación de firma digital.

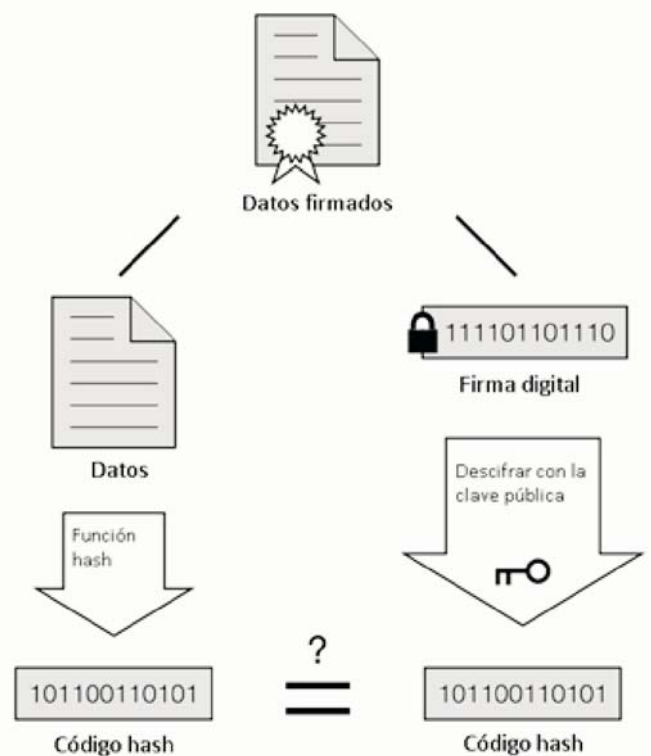
Cerbero efectúa varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante.
- Revocación del certificado digital del firmante (puede ser por o ).
- Inclusión de sello de tiempo.

La utilización del sistema de Directorio Activo como único servicio corporativo de gestión de servicios a personas tanto en los sistemas de seguridad electrónica y de los sistemas de seguridad lógica de acceso, al medio, permite establecer una perfecta sincronización entre ambos sistema. Gracias a la sinergia que se genera entre ambos sistemas.

**Cerbero** incorpora en un terminal compacto y ergonómico una pantalla táctil emulando un teclado QWERTY, un terminal de lectura de tarjetas inteligentes y un terminal biométrico de huella dactilar todo ello conformando un dispositivo con diseño de líneas rectas robusto y moderno para completar el lector de triple tecnología.

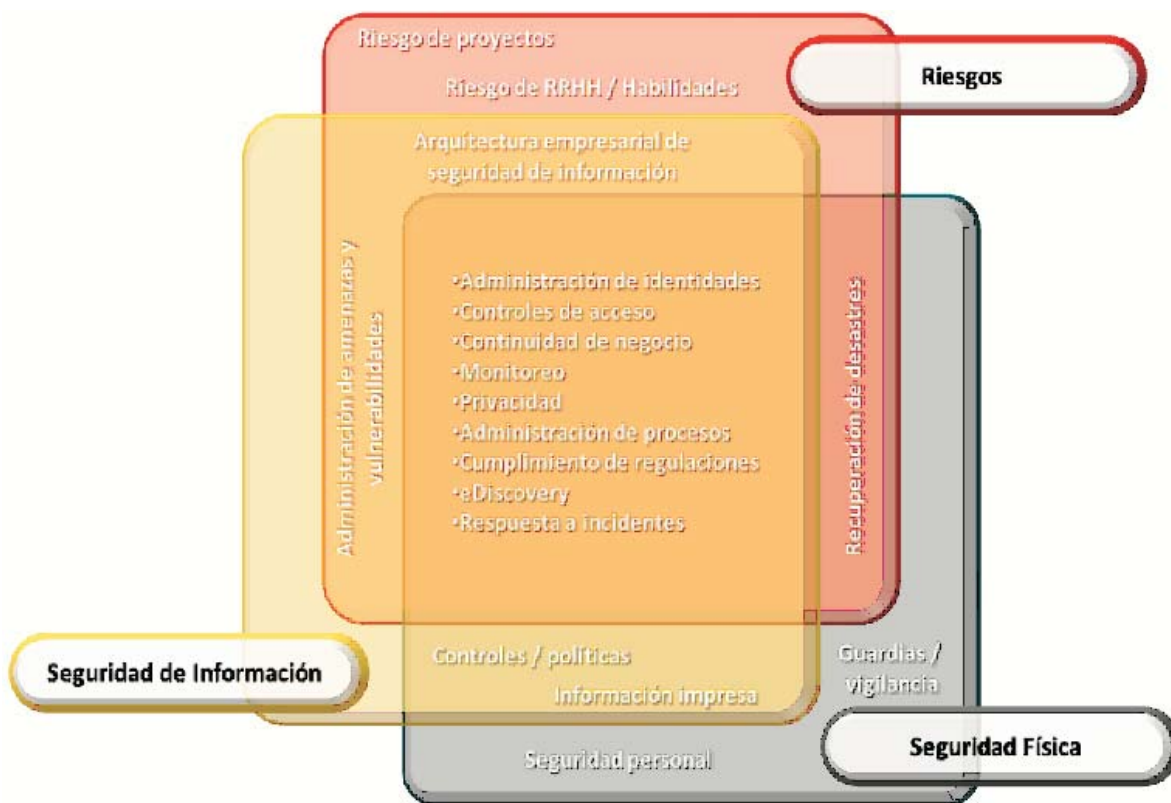
### Comprobación de una Firma



La eficiencia y fiabilidad del sistema se hace máxima al permitir la gestión de bases de datos de usuarios autorizados y revocados de un modo dinámico sobre los servicios de directorio activo.

**Cerbero** verifica y comprueba, una vez identificado inequívocamente el usuario a partir de sus datos biométricos contrastados con su firma digital y su contraseña alfanumérica de acceso al medio, que se encuentra autorizado a acceder al área protegida.

La gestión de permisos y privilegios de acceso a un área se convierte en algo tan simple para el administrador del sistema, como la acción de dar autorización para uso de una impresora o permisos de acceso a los ficheros en un servidor. Un único punto de gestión y un único entorno tras la **sinergia establecida** entre el **Servicio de Directorio Activo** y el **Servicio de Control de Accesos**.



## Historia

Desde la primera generación de Cerbero la evolución ha consistido en tres aspectos fundamentales: aumento de la seguridad, optimización de los tiempos de verificación e integración de nuevos requisitos dentro de todo diseño de seguridad física y lógica para una instalación crítica como puede ser un CPD.

Brevemente podemos distinguir tres hitos primordiales en la evolución de Cerbero:

- **1ª Generación:** la primera generación de Cerbero desarrollada por ACAL BFI IBERIA, externamente no aparentaba ser muy diferente de un terminal biométrico con tarjeta y teclado como tantos otros del mercado. La diferencia fundamental era que en su interior encerraba un procesador de última generación en el cual residía el procedimiento funcional que enlazaba su operativa a la base de datos del sistema de control de accesos y al directorio activo del sistema de seguridad lógica.
- **2ª Generación:** Pronto surgió la idea de la primera mejora en el sentido de usar contraseñas alfanuméricas en lugar de un código numérico. Para ello se hacía necesario dotar al terminal de un terminal ampliado que permitiera la introducción de la contraseña de un modo cómodo y que no requiriera la repetición de teclas numéricas como si fuera un teléfono móvil. El avance actual del mercado en pantallas táctiles permitió implementar esta prestación.
- **3ª Generación:** Conseguida la ergonomía del sistema y la optimización de los tiempos se adecuó el diseño de la envolvente en un terminal fácil y cómodo de usar. Se le incorporó a Cerbero unas instrucciones de uso en la propia pantalla claras y sencillas, las cuales permiten al usuario no experimentado saber, sin lugar a dudas, la operativa a seguir en el proceso de identificación requerido. **Cerbero 3ª Generación** acababa de nacer como la evolución en su máximo grado de un producto altamente contrastado y con la operativa más robusta y segura del mercado.

## Funcionamiento

De modo esquemático y resumido podemos representar los dos criterios de acceso (acceso de personas y acceso al medio) usados por los sistemas de seguridad lógica y seguridad física y cómo **Cerbero** los aúna en un único entorno.

Con el objetivo de realizar la autenticación de usuarios bajo un único sistema de control de accesos se ha planteado un sistema que cumpla las especificaciones de seguridad mediante tres tipos de tecnologías (Huella dactilar y Firma digital) y contraseña digital.



Para las tecnologías de autenticación basadas en la huella dactilar y huella digital los datos relativos a los usuarios son tramitados a través del directorio activo del cliente. Se obtendrán así los permisos relativos a los usuarios mediante una consulta especializada. La adquisición de los datos del directorio activo podrá realizarse mediante consultas manuales o automáticas (tareas programadas).

Los datos referentes a los usuarios obtenidos del directorio activo son reestructurado e introducidos al sistema de control de accesos. El sistema permitirá que cada usuario tenga 11 credenciales, 10 de ellas son vinculadas a sus huellas dactilares y la última credencial se relaciona con la firma electrónica.

Los datos referentes a las huellas son almacenados en el lector y en la base de datos del sistema de gestión de accesos.

En el modo acceso mediante tarjeta con certificado mediante comandos ADPU y PDUs, el lector discrimina entre tipos de certificados (X.509), verificando si el certificado fue emitido por la entidad esperada.

En el mismo instante que se procesa la tarjeta (hash, SHA, MD5 ) el lector abrirá una pantalla de diálogo, donde se introducirá la contraseña alfanumérica correspondiente a la tarjeta inteligente. Mientras se introduce dicha contraseña, el lector

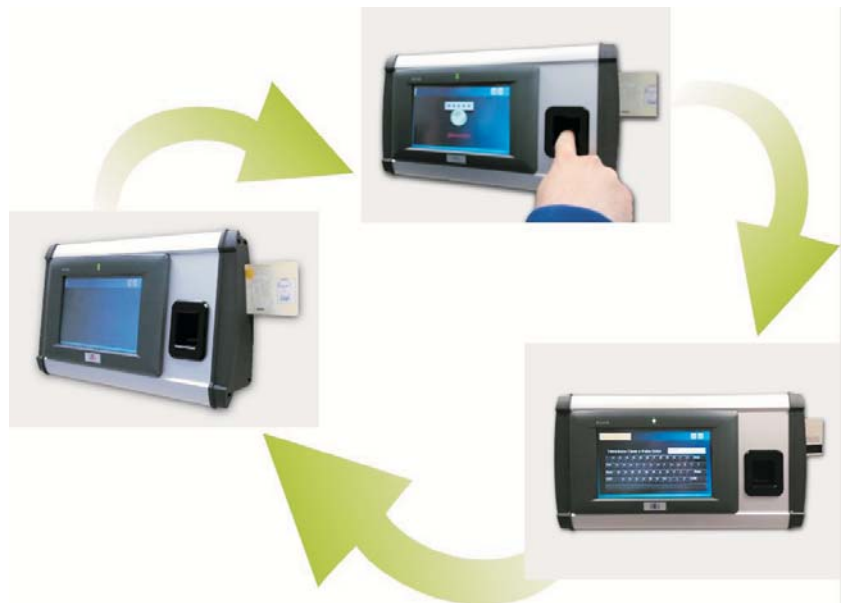
comprueba si el certificado en uso se encuentra revocado en el directorio activo.

Si el certificado no está revocado mediante la solicitud al servidor, "CLR" del listado de certificados revocados y además la comprobación de la contraseña introducida. El lector enviará el código referente a la credencial del usuario, permitiendo el acceso al área protegida.

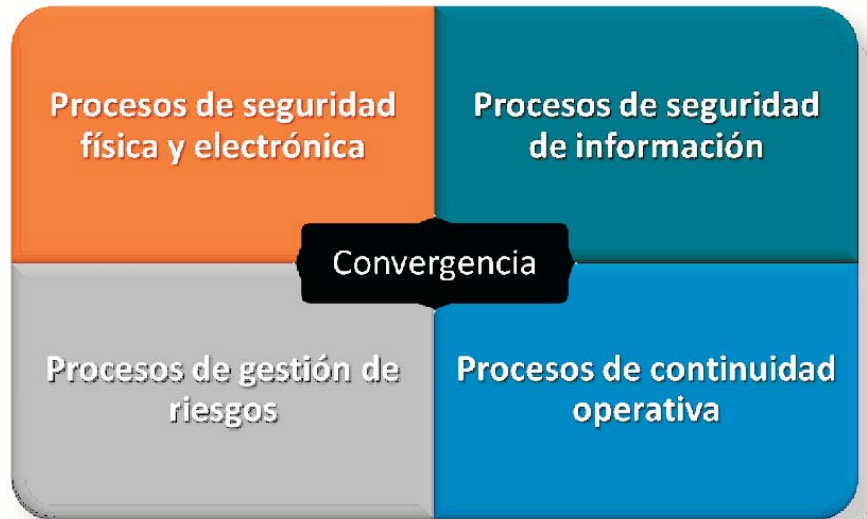
### Ventajas y beneficios

Ante un mercado globalizado donde predomina el uso de la tecnología y riesgos de alta criticidad que generan importantes pérdidas; la convergencia entre la seguridad física y lógica que conjuga **Cerbero**, permite afrontar estos eventos bajo esquemas de sinergia, eficiencia y efectividad.

Por otro lado, **Cerbero** permite importantes sinergias orientadas a la reducción de costos por el uso de tecnología, mayor capacidad de reacción inmediata, optimizar el rol preventivo y adecuado manejo de estrategias.



La convergencia entre la seguridad lógica y física del terminal **Cerbero**, permite garantizar la continuidad operativa de los procesos establecidos en seguridad física en general y en particular en seguridad electrónica pero además garantiza la continuidad operativa y metodológica de los procesos de seguridad de la información y simplifica enormemente la gestión de riesgos al fusionar en un entorno de identificación absolutamente inviolable las últimas tecnologías en identificación digital y biométrica.



Todo ello convierte a Cerbero en la solución de seguridad ideal para instalaciones críticas con una importante implantación a día de hoy en el diseño de sistemas de seguridad física y lógica en CPDs en nuestro país.

### Departamento de I+D

En el año 2005 ACAL BFI IBERIA inicia una nueva andadura en el campo de la investigación y el desarrollo, creando el Departamento de I+D. Inmersos en nuestro afán de superación dotamos a nuestro departamento de un alto capital humano y amplios medios técnicos e innovadores.

Esta estructura transformó la propuesta de valor de la compañía que pasó a ofertar a sus clientes instaladores una potente solución global integradora de los productos líderes en distintas tecnologías.

Así se creó IPNOVA, la plataforma de integración bajo el paraguas del estado del arte. Diseñada y desarrollada íntegramente por ACAL BFI IBERIA para dar satisfacción a los requerimientos de cada instalador en cada instalación.

La implementación paulatina de la consultoría tecnológica en los distintos clientes con el paso del tiempo ha dado paso al desarrollo de más de 50 nuevos productos introducidos en el mercado de la seguridad electrónica como el que nos ocupa en el presente documento.



C/ Anabel Segura 7 Planta de Acceso  
28108 - Alcobendas (Madrid)

Teléfono: 914531160  
Fax: 91 662 68 37

Innovación Española 