centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo F.14: Sistemas de Gestión de Bases de Datos (DBMS)

Julio de 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.17 12:25:48 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023
NIPO: 083-23-071-5

Fecha de Edición: julio de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Sistemas de Gestión de Bases de Datos (DBMS, *DataBase Management System*)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado, desde el punto de vista de la seguridad, para ser empleado en los sistemas de información del sector público para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS)**. Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
    - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
    - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
    - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Sistemas de Gestión de Bases de Datos (DBMS**) conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Se considera **Sistema de Gestión de Bases de Datos (DBMS)** a todo producto destinado al manejo de bases de datos, cuya función principal sea la de servir de interfaz entre la base de datos, el usuario y las distintas aplicaciones utilizadas en la organización.
7. Generalmente se trata de productos software que facilitan el uso y manipulación de las bases de datos de forma segura, sencilla y ordenada. El DBMS proporciona a los usuarios una forma sistemática de crear, recuperar, actualizar y administrar los datos, asegurando que los datos estén organizados de manera consistente y permanezcan fácilmente accesibles. Además, proporciona una vista centralizada de datos a los que pueden acceder múltiples usuarios, desde múltiples ubicaciones, de manera controlada.
8. Un DBMS debe tener la capacidad de limitar el acceso a los datos y otros objetos de la base de datos bajo su control, únicamente a los usuarios autorizados. Y también debe registrar todas las acciones realizadas por los usuarios, en los correspondientes registros de auditoría.
9. Además de las características anteriormente indicadas, los DBMS pueden tener alguna de las siguientes capacidades:
    - Interacción con el Sistema Operativo subyacente para recuperar y presentar los datos bajo su gestión.
    - Indexación de los datos, es decir, la capacidad de vincular el dato con su ubicación física. Esto permite la recuperación rápida del dato cuando se lanzan consultas basadas en un valor o rango de valores.
    - Programación de scripts para automatización de tareas rutinarias a realizar en la base de datos como, por ejemplo, *backups*.
    - Mecanismos de concurrencia que permiten acceso simultáneo a los datos, a múltiples usuarios.
    - Uso de Lenguajes de Manipulación de datos o *Data Manipulation Languages* (DML) para la realización de consultas y manipulación de datos. Por ejemplo, el DML más utilizado para gestionar datos en bases de datos relacionales es SQL (*Structured Query Language*).
    - Provisión de un modelo de datos con el que se puedan definir objetos y conceptualizar las estructuras y la organización de los datos (por ejemplo, modelos de datos relacionales, jerárquicos y orientados a objetos).
10. Generalmente, un DBMS soporta dos tipos de usuarios:
    - Usuarios que interactúan con el DBMS para consultar y/o modificar objetos y datos para los que están autorizados.

- Administradores autorizados que instalan, configuran y administran las bases de datos e implementan políticas relacionadas con la información de la organización gestionada por dichas bases de datos. Por ejemplo, políticas de acceso, integridad, consistencia o disponibilidad de los datos.

11. Generalmente, un DBMS almacena y gestiona dos tipos de datos:

    - Datos de usuario que el DBMS mantiene y protege. Por ejemplo: datos almacenados por el usuario, definiciones de dichos datos (metadatos), consultas (*querys*), funciones o procedimientos generados por el usuario.
    - Datos que el propio DBMS utiliza para operar la base de datos. Por ejemplo: parámetros de configuración, atributos de seguridad de los usuarios, logs de transacciones, registros de auditoría.

2.2 CASOS DE USO

12. Dada la naturaleza y el objetivo de este tipo de productos, existen multitud de arquitecturas y, por lo tanto, casos de uso posibles. A continuación, se indican los más comunes, aunque no son limitantes.

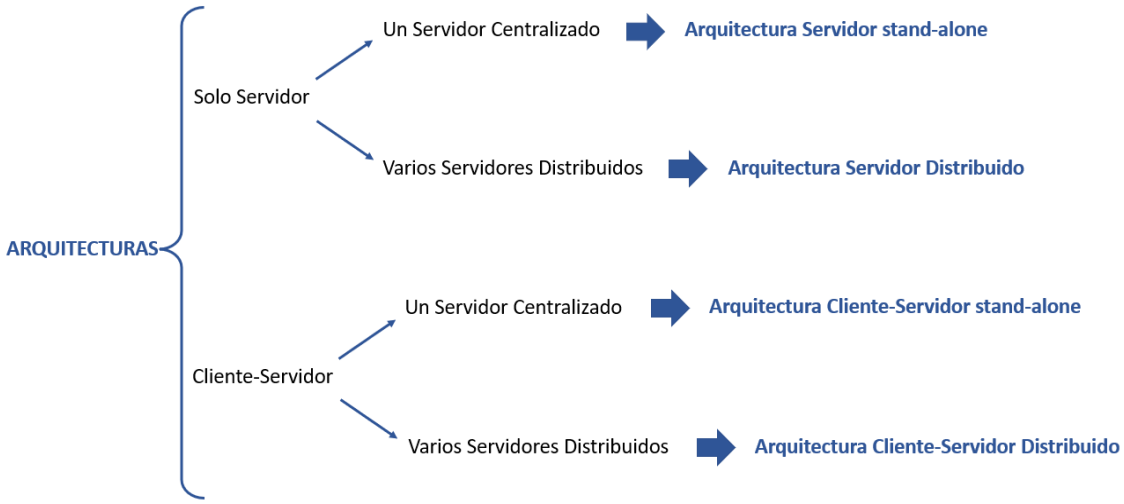

Figura 1 – Resumen de Arquitecturas

2.2.1. CASO DE USO 1 – ARQUITECTURA SERVIDOR STAND-ALONE

13. La arquitectura del producto está formada por una única instancia del Servidor DMBS (*stand-alone*). Dicho servidor es un *software* que se instala y despliega en un dispositivo *hardware* de propósito general con un sistema operativo compatible.
14. No existe Cliente DBMS. Los usuarios y aplicaciones interactúan directamente con el *DMBS Server* a través de los interfaces ofrecidos por este.

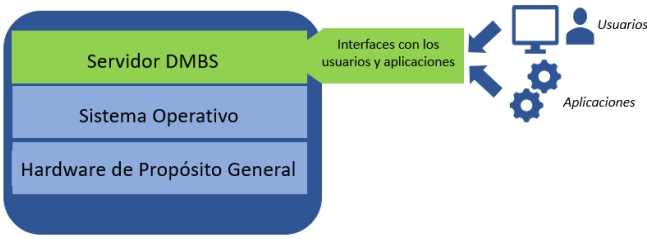

Figura 2 – Arquitectura Servidor *stand-alone*

2.2.2. CASO DE USO 2 – ARQUITECTURA SERVIDOR DISTRIBUIDO

15. La arquitectura del producto está formada por varias instancias del Servidor DMBS. Dichos servidores consisten en *software* que se instala y despliega en dispositivos *hardware* de propósito general con un sistema operativo compatible.
16. No existe Cliente DBMS. Los usuarios y aplicaciones interactúan directamente con los DMBS Server a través de los interfaces ofrecidos por estos.

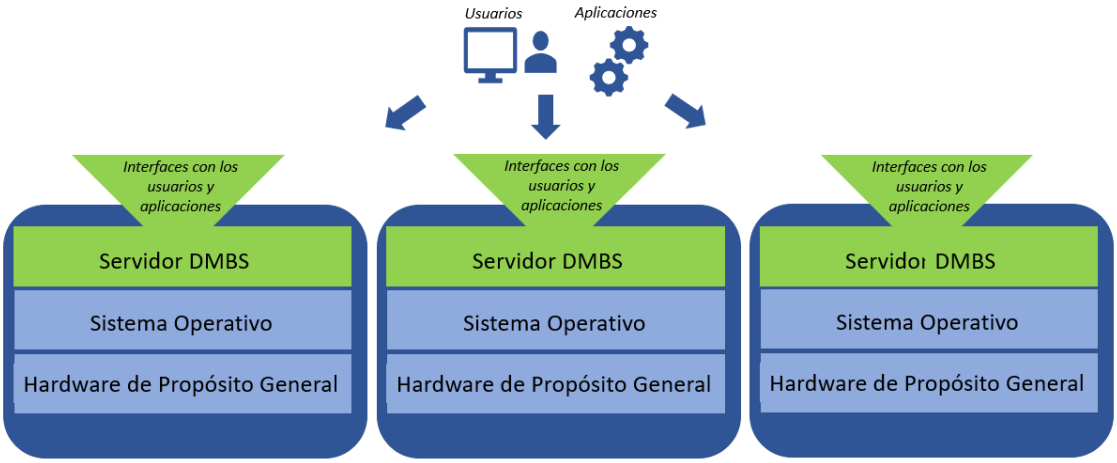

Figura 3 – Arquitectura Servidor Distribuido

2.2.3. CASO DE USO 3 – ARQUITECTURA CLIENTE-SERVIDOR *STAND-ALONE*

17. La arquitectura del producto está formada por:
    - Una única instancia del Servidor DMBS (*stand-alone*). Dicho servidor es un *software* que se instala y despliega en un dispositivo *hardware* de propósito general con un sistema operativo compatible.
    - Uno o varios Clientes DBMS que se comunican simultáneamente con el servidor DMBS. Los clientes pueden ser aplicaciones *software* instaladas en los equipos de usuario con su propio sistema operativo, o clientes ligeros (*thin clients*). Los clientes se pueden conectar con el servidor DBMS directamente, o a través de una LAN.

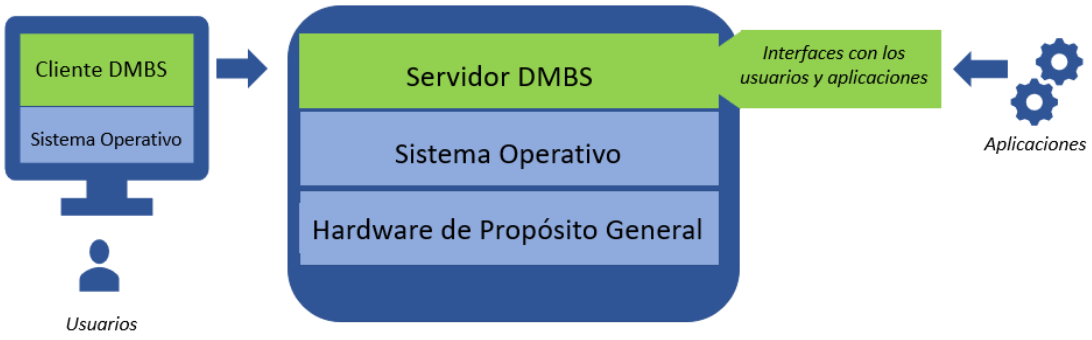

Figura 4 – Arquitectura Cliente-Servidor *stand-alone*

2.2.4. CASO DE USO 4 – ARQUITECTURA CLIENTE-SERVIDOR DISTRIBUIDO

18. La arquitectura del producto está formada por:

- Varias instancias del Servidor DMBS. Dichos servidores consisten en software que se instala y despliega en dispositivos hardware de propósito general con un sistema operativo compatible.
- Uno o varios Clientes DBMS que se comunican simultáneamente con los servidores DMBS. Los clientes pueden ser aplicaciones software instaladas en los equipos de usuario con su propio sistema operativo o clientes ligeros (*thin clients*). Los clientes se pueden conectar con los servidores DBMS directamente o a través de una LAN.

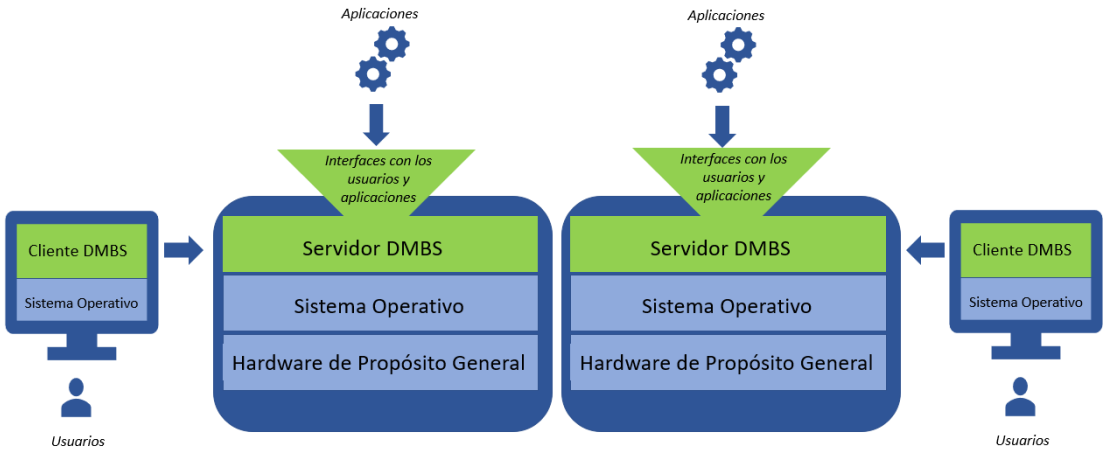

Figura 5 – Arquitectura Cliente-Servidor distribuido

2.3 ENTORNO DE USO

19. Para la utilización en condiciones óptimas de seguridad de los Sistemas de Gestión de Bases de Datos (DBMS), es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física**. El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
    - **Administración confiable:** Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
    - **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas. Además, el administrador deberá garantizar la autenticidad e integridad de dichas actualizaciones.
    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de gestión de la base de datos e interfaz entre la base de datos, los usuarios y las aplicaciones como función principal, y no debe proporcionar ninguna otra funcionalidad o servicio.
    - **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
    - **Plataforma confiable.** En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

20. Si existe cliente DBMS, suele presentarse como una aplicación *software* a instalar sobre un dispositivo con sistema operativo compatible, o un cliente ligero que accede al servidor DBMS a través de alguna aplicación que actúa como *proxy*.
21. El Servidor DBMS suele presentarse como un *software* que se instala y despliega en dispositivos *hardware* de propósito general con un sistema operativo compatible.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

22. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).

23. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.

24. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria.* Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.

25. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

26. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una evaluación **STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

27. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

    - **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
    - **AC.PSS**. Datos de configuración, registros de auditoría y cualquier dato que el propio DBMS utilice para operar la base de datos, y que deben ser protegidos en Integridad.
    - **AC.UserData**. Datos y objetos de usuario que el DBMS mantiene y protege en confidencialidad e integridad.

3.2 AMENAZAS

28. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección 2.2, serían:

- **A.NOAUT Acceso no autorizado de administrador**: Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles**: Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.AUD Actividades no detectadas**: Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CON Compromiso de credenciales**: Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.RECURSOS:** Un atacante puede obtener un acceso no autorizado a los objetos de la base de datos mediante la reasignación (*reallocation*) de recursos de un usuario o proceso, a otro.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

29. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 PERFIL DE PROTECCIÓN

30. **REQ.1**. Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Database Management Systems (DBMS PP) Base Package	*2.12*	*05/04/2017*	*DBMS Working Group / Technical Community*
Collaborative Protection Profile (cPP) for Database Management Systems	*1.3*	*21/06/2023*	*Database Management System iTC*

31. **REQ.2**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) del *Protection Profile for Database Management Systems (DBMS PP) Base Package* V.2.12 con un nivel de confianza EAL (*Evaluation Assurance Level*) EAL2 o superior.

4.2 CRIPTOGRAFÍA

32. El siguiente requisito podrá ser cubierto por el producto o por su entorno operacional (por ejemplo, el sistema operativo).

33. **REQ. 3**. Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

4.3 CANALES SEGUROS

34. Podrán ser cubiertas por el producto o por su entorno operacional.

35. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior;*

DTLS; HTTPS/TLS 1.2 o superior] con los siguientes mecanismos criptográficos [***asignación**: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

36. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.
37. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.
38. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación**: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
DBMS	DataBase Management System (Sistema de Gestión de Bases de Datos)
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
SCL	Servidor de Control de Llamadas
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*