centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 499

Arquitecturas de seguridad para servicios en la nube

Noviembre 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-291-0.

Fecha de Edición: noviembre de 2022

CCN 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
2022.11.21 18:19:51 +01'00'

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Noviembre de 2022

Esperanza Casteleiro Llamazares
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. La evolución actual de las Tecnologías de la Información y las Comunicaciones (TIC) demanda cada día más capacidad de computación y almacenamiento, disponibilidad, movilidad o incluso ubicuidad y compartición de información. En un momento en el que ya no se concibe que prácticamente ningún servicio se encuentre aislado ni anclado a una ubicación física, emerge fuertemente la necesidad de consumir servicios en la nube, básicamente porque aportan las siguientes ventajas, que se adaptan perfectamente a las necesidades actuales:

    a) **Escalabilidad de recursos**. Los servicios que se contratan en la nube a un Proveedor de Servicios en la Nube (CSP, por sus siglas en inglés) presentan la ventaja de ser escalables. De hecho, estos CSP suelen ofrecer distintas formas de contratación que permiten pago por uso, realizar una reserva de recursos con unas determinadas capacidades, o distintas combinaciones de ambos. En las arquitecturas tradicionales *on premise*, existen riesgos de infradimensionar el Sistema y tener problemas de caída de servicio por saturación en picos de trabajo o sobredimensionarlo, lo que supondría una infrautilización que supondría desperdiciar parte de la inversión realizada en infraestructura. Con los servicios en la nube estas decisiones y riesgos asociados desaparecen.

    b) **Disponibilidad de recursos**. Hoy en día los servicios en la nube permiten acceder a los recursos desde cualquier ubicación con una disponibilidad casi absoluta. Esto contrasta fuertemente con los servicios *on premise*, que en muchos casos necesitan desplegar costosas infraestructuras para poder ofrecer un nivel de capilaridad aceptable y llegar a todos sus usuarios.

    c) **Despliegue dinámico de arquitectura**. Dado que es el proveedor del servicio el que despliega la arquitectura y el consumidor solamente paga por su uso, no es necesario realizar grandes inversiones para desplegar una arquitectura determinada y es igualmente sencillo implementar cambios profundos dentro de la arquitectura para adaptarse a las necesidades cambiantes sin que ello suponga un coste inasumible. En los sistemas *on premise* suelen hacerse grandes inversiones a la hora de desplegar un sistema que deben ser rentabilizadas antes de realizar cambios profundos. Esto impide, en ocasiones, realizar adaptaciones dinámicas e incluso depender de sistemas *legacy* considerados ineficientes o inseguros.

2. No obstante, este cambio de paradigma trae asociados cambios también en el diseño de las arquitecturas de seguridad que protegen los activos de los usuarios, especialmente si se trata de Información Clasificada. Estos cambios están basados en:

    a) **Modificación del perímetro**. Uno de los pilares fundamentales de las arquitecturas de seguridad de sistemas *on premise* es la protección del perímetro y de los flujos de información intercambiados, especialmente en el ámbito de los sistemas clasificados. En este nuevo paradigma el perímetro se amplia y se desdibuja hasta tal punto que es prácticamente imposible

delimitarlo, por lo que la protección recae en el propio dato. Esto no quiere decir, ni mucho menos, que el perímetro haya dejado de protegerse o puedan relajarse dichas medidas de protección, únicamente que el perímetro pasará a ser el propio dato cuando no pueda determinarse otro mayor. Es lo que hoy se conoce como el paradigma de Seguridad Centrada en el Dato o *Data Centric Security*, del cual los servicios en la nube son un caso particular.

b) **Pérdida de gobierno del dato**. En los sistemas *on premise*, el propietario del Sistema y de la información suele ser el mismo, por lo tanto, es el único responsable de proteger su información. En los servicios en la nube, el acceso y la custodia de dicha información se delega a un tercero. Por lo tanto, será necesario analizar qué tipo de información y en qué condiciones es posible realizar esta delegación. Este aspecto adquiere especial relevancia en el ámbito de la información clasificada.

c) **Aislamiento de datos.** La tenencia múltiple y la compartición de recursos son características inherentes de la computación en la nube. Esto incrementa el riesgo de divulgación no autorizada de información por fallos de separación en el almacenamiento, la memoria, el enrutado, etc.

3. Por lo tanto, es necesario analizar qué medidas debe implementar la arquitectura de seguridad de un servicio en la nube para posibilitar el manejo de información sensible o clasificada (siempre que sea viable o hasta un grado determinado).

2. OBJETO

4. El presente documento tiene como objetivo definir las **medidas de seguridad** asociadas a las fases de **diseño** e **implementación** de una **arquitectura de seguridad** para sistemas de información que ofrecen servicios en la nube. Por lo tanto, quedan fuera del alcance del presente documento la definición de todas aquellas medidas de seguridad y procedimientos que tengan impacto únicamente en las fases de operación y mantenimiento, para las cuales se aplicará la normativa que sea de aplicación.
5. En concreto, para la arquitectura mencionada, se determinarán las medidas de seguridad asociadas a los diferentes grados de **Información Clasificada, ya sea nacional o procedente de ámbitos internacionales.**
6. A la hora de interpretar este documento es importante tener en cuenta las siguientes consideraciones:
   a) Las arquitecturas planteadas deben tomarse como un conjunto de soluciones que dan respuesta a la necesidad de utilizar servicios en la nube cuando se maneja información que, por sus características, requiere de medidas especiales de protección. **En ningún momento deben tomarse como un conjunto exclusivo y limitante de soluciones**, ya que pueden existir otras alternativas igualmente válidas que cumplan con los requisitos establecidos por la normativa vigente para cada ámbito y que deberán analizarse caso por caso.
   b) Como se verá en apartados posteriores, los servicios en la nube adoptan un modelo de responsabilidad compartida en el que pueden existir diferentes actores con diferentes responsabilidades. En este documento se han resumido en dos: cliente y proveedor. Se asume que el primero es el organismo que consume el servicio y el segundo el que lo ofrece, total o parcialmente. En caso de existir más actores deberá analizarse qué medidas de las planteadas son responsabilidad de cada uno.
   c) Todas las medidas de seguridad recogidas en el presente documento están definidas desde el punto de vista del cliente. Es decir, **el cliente deberá implementar aquellas medidas que se definan bajo su responsabilidad y exigir al proveedor cuando contrata el servicio que cumpla con las definidas bajo responsabilidad del proveedor**. Por lo tanto, **no se han detallado aquellas medidas que debe implementar el proveedor sobre las cuales no tiene visibilidad el cliente, ya que se suponen garantizadas por las distintas auditorías de seguridad a las que se debe somenter el proveedor del servicio y que el cliente debe exigir**, tal como se detallará en apartados sucesivos.

3. ESTRUCTURA DEL PRESENTE DOCUMENTO

7. El presente documento se estructura en los siguientes apartados:

   a) **Apartado 4. Conceptos básicos de servicios en la nube**. En este apartado se presentan los distintos modelos de despliegue y categorías de servicio comúnmente utilizados cuando se habla de servicios en la nube.

   b) **Apartado 5. Objetivos de seguridad.** En este apartado se presentan los objetivos de seguridad a alto nivel que deben satisfacer las medidas de seguridad en cada una de las arquitecturas descritas en el presente documento.

   c) **Apartado 6. Medidas de seguridad**. En este apartado se describen, de manera genérica, todas las medidas de seguridad que pueden utilizarse de cara a satisfacer los objetivos de seguridad descritos en el apartado 5.

   d) **Apartado 7. Análisis de arquitecturas**. En él se describen los diferentes tipos de arquitecturas que se van a considerar en este documento, junto con sus principales características técnicas.

   e) **Apartado 8. Definiciones**. En este apartado se incluyen definiciones de utilidad para el entendimiento de este documento.

   f) **Apartado 9. Referencias**.

   g) **Apartado 10. Abreviaturas**

4. CONCEPTOS BÁSICOS DE SERVICIOS EN LA NUBE

4.1 MODELOS DE DESPLIEGUE

8. Se pueden clasificar las infraestructuras de la nube en públicas, privadas, comunitarias o híbridas.

   a) **Nube pública.** La infraestructura de esta nube está mantenida y gestionada por terceras personas no vinculadas con la organización proporcionando recursos de forma abierta a entidades heterogéneas, sin más que un contrato con el mismo proveedor que controla dicha infraestructura.

   b) **Nube privada.** La infraestructura de esta nube o servicios provistos son completamente dedicados para un solo cliente que controla qué aplicaciones debe ejecutarse y dónde (infraestructura bajo demanda). Puede ser propiedad, ser administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

      La nube pública presenta flexibilidad de contratación y la nube privada, en la mayoría de los casos, exige determinados compromisos de consumo o permanencia.

   c) **Nube híbrida.** Los servicios se ofrecen de forma pública y privada. Un usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.

   d) **Nube comunitaria.** La infraestructura de esta nube o servicios provistos son compartidos en comunidad cerrada por varias organizaciones relacionadas entre ellas y que comparten requisitos con la finalidad de servir a una función o propósito común (seguridad, política…).

      La nube comunitaria puede ser propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas.

4.2 CATEGORÍAS DE SERVICIO

9. Se ofrecen una serie de categorías de servicio que se detallan a continuación:

   a) **IaaS (*Infrastructure as a Service*).** Se encarga de entregar una infraestructura al usuario, proporcionando recursos de procesamiento y almacenamiento a través de la red, sin ningún otro valor añadido (servicios de uso de almacenamiento, *hardware*, servidores y componentes de red).

      El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red.

   b) **PaaS (*Platform as a Service*).** Se encarga de entregar una plataforma a la organización cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.

Se proporcionan herramientas y utilidades para desarrollar aplicaciones sobre la nube como bases de datos o entornos de programación en las que el usuario puede desarrollar sus propias soluciones.

c) **SaaS (*Software as a Service*).** Modelo de distribución de *software* en el que las aplicaciones están alojadas por un proveedor de servicio y puestas a disposición de los usuarios a través de red.

El usuario encuentra en la nube las herramientas con las que puede implementar los procesos necesarios: aplicaciones ofimáticas, correo electrónico, etc… donde el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza.

10. Por lo tanto, en todas las categorías de servicio los aspectos relacionados con la conformidad y la seguridad son una responsabilidad compartida entre el proveedor o CSP (*Cloud Service Provider*) y el cliente o CSC (*Cloud Service Customer*), tal como se muestra en la siguiente figura:

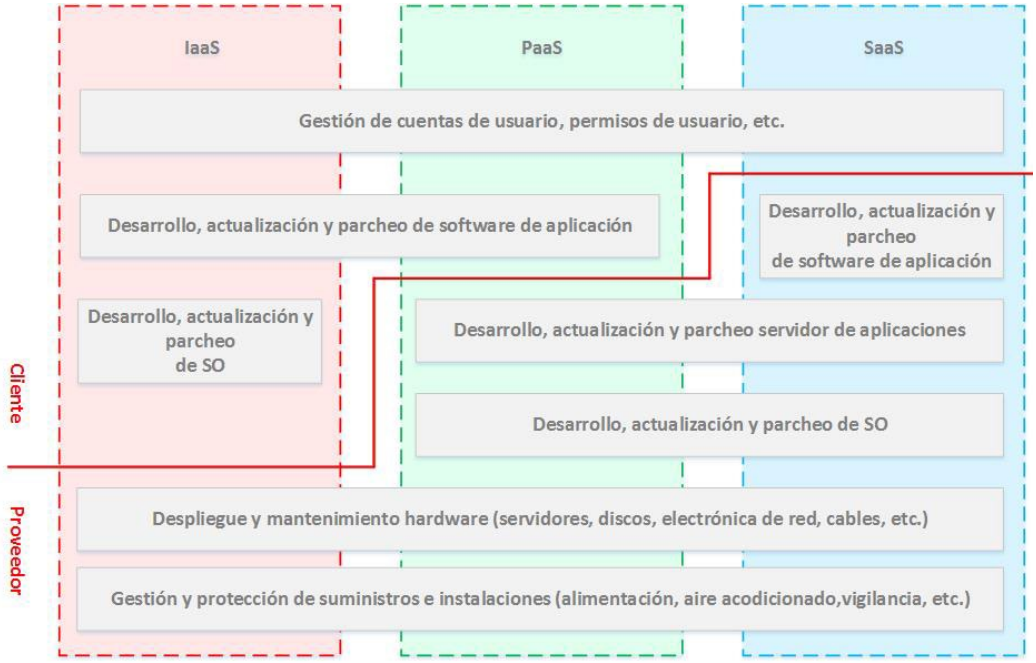


Figura 1. Modelo de responsabilidad compartida

11. Así, podemos hablar de seguridad *"de"* la nube y seguridad *"en"* la nube:

a) **Seguridad de la nube.** el CSP será responsable de la seguridad de los servicios que provea al cliente, así como de cumplir aquellos acuerdos de nivel de servicio que establezca. Abarcará la seguridad del hardware, el software, las redes y las instalaciones que ejecutan servicios en la nube.

b) Seguridad en la nube. La responsabilidad del cliente estará limitada a la seguridad de los servicios que despliegue sobre la nube que no sean propietarios del CSP, así como de las configuraciones que establezca, en base a sus capacidades dependiendo de la categoría del servicio que haya contratado.

5. OBJETIVOS DE SEGURIDAD

12. A continuación, se detallan los **objetivos de seguridad** para la arquitectura objeto de diseño:

a) **Protección de la información**. El servicio en la nube deberá tener la capacidad de manejar de manera segura información sensible o clasificada que demande protección en cualquiera de sus dimensiones de seguridad, en su almacenamiento, procesamiento y transmisión. Para ello, deberá implementar:

- **Control de los flujos de información:** Los flujos de información estarán restringidos, físicamente o mediante configuración *software*, a las interfaces habilitadas. Se protegerá la confidencialidad, integridad y autenticidad y se impedirá el establecimiento de canales encubiertos que faciliten la transmisión no autorizada de información.

- **Aislamiento de datos**. La tenencia múltiple y la compartición de recursos son características inherentes de la computación en la nube. El servicio deberá garantizar la separación de los recursos asignados al usuario, de forma que no se produzca trasvase de información entre recursos, salvo que esté debidamente autorizado, en cuyo caso deberán estar controlados y monitorizados.

- **Acceso autorizado a la información**. El servicio debe garantizar el acceso a la información únicamente al personal que esté debidamente autorizado.

b) **Protección del servicio**. El servicio deberá protegerse de ataques (actualizaciones no permitidas, *malware*, etc.) que puedan alterar su correcto funcionamiento y en especial sus funcionalidades de seguridad críticas, así como de ataques que puedan afectar a su disponibilidad.

c) **Cumplimiento normativo.** El Sistema deberá implementar medidas orientadas a comprobar la efectividad de las prácticas de gestión de datos del proveedor y verificar que dichas prácticas están de acuerdo a lo establecido en la ley.

6. MEDIDAS DE SEGURIDAD

13. A partir de las categorías de servicio definidas en la sección 4.2, en la cual se establece un **modelo de responsabilidad compartida** en dos (2) niveles (CSC y CSP), se definen medidas de seguridad que podrán estar asociadas al cliente, al proveedor o a ambos, sin perjuicio de otras medidas que deban aplicarse cuando la información que se vaya a manejar tenga una normativa de seguridad específica (ENS, Clasificada, RGPD, etc).
14. A continuación, se detallan las medidas de seguridad que deben implementarse, que se han agrupado en 17 dominios técnicos.

6.1 DOMINIO 1 (D1): AUDITORÍA Y ASEGURAMIENTO

15. Este dominio de seguridad recoge aquellas medidas relativas al cumplimiento de las políticas de seguridad de la organización, así como a los requisitos exigibles por la legislación/regulación vigente.

6.1.1 AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI)

16. En esta medida se describen las actividades de auditoría que deben realizarse de cara a acreditar la seguridad del sistema de información que presta el servicio en la nube. A lo largo de este proceso de acreditación se auditarán todas aquellas medidas que sean aplicables, atendiendo al tipo de información que vaya a manejar el sistema.

6.1.2 SOMETIMIENTO JURISDICCIONAL (SJD)

17. En esta medida se recogen los requisitos relativos a la jurisdicción a la que debe someterte, tanto el CSP como el CSC.

6.2 DOMINIO 2 (D2): SEGURIDAD DE APLICACIONES E INTERFACES

18. Este dominio de seguridad recoge aquellas medidas relativas a la seguridad del *software* de aplicación que se ejecuta o está siendo desarrollado en el entorno en la nube.

6.2.1 CUALIFICACIÓN DE SERVICIO EN LA NUBE (CSN) Y CUALIFICACIÓN DE PRODUCTO (CPN).

19. Bajo esta medida se recogen los requisitos relativos a las garantías de seguridad ofrecidas por los productos/servicios de seguridad derivadas de haber superado con éxito un proceso de evaluación y certificación.
20. En este sentido, el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) [2] ofrece un listado de referencia para los Organismos del Sector Público en la adquisición de productos y servicios de seguridad que ofrecen unas garantías mínimas determiandas por el CCN. El **CPSTIC** se divide en **Productos y Servicios**

Cualificados (orientados a sistemas que manejen información sensible) y **Productos y Servicios Aprobados** (orientados a sistemas que manejan información clasificada). Bajo esta medida, se recogen los requisitos de cualificación del servicio en la nube o del producto que se despliegue en esta. Además, dentro del CPSTIC también se recogen las referencias a los **Procedimientos de Empleo Seguro (PES)** que deben utilizar para configurar los servicios o productos de forma segura.

6.2.2 APROBACIÓN (ASN Y APN)

21. Bajo estas medidas se recogen los requisitos de aprobación de productos (APN) y servicios en la nube (ASN).

6.3 DOMINIO 3 (D3): GESTIÓN DE CONTINUIDAD Y RESILIENCIA DE OPERACIONES

22. Este dominio de seguridad se refiere a la implementación de medidas orientadas a asegurar la continuidad de negocio, así como los procedimientos de resiliencia y recuperación ante desastres.

6.3.1 ACUERDO DE SERVICIO (SLA)

23. Bajo esta medida se definirán los acuerdos a los que se llegue entre el CSC y el CSP relativos a:

a) **Disponibilidad del sistema**. Establecimiento de ratios de disponibilidad que el proveedor de servicio deberá asumir, determinación de tiempos máximos de respuesta, recuperación, etc. Con los acuerdos a nivel de servicio, el CSP se debe comprometer a ofrecer información vinculante, comprensible y transparente relativa a:

- Disponibilidad de servicio.
- Categoría y priorización de incidentes.
- Tiempos de respuesta ante caídas de la operación normal, de acuerdo a la categorización (tiempo transcurrido entre que se reporta y se resuelve el incidente).
- Tiempo de recuperación (tiempo transcurrido hasta que el incidente ha sido resuelto). Se diferencian distintos parámetros:
    i. Máximo tiempo de caída tolerable / Objetivo de tiempo de recuperación (RTO).
    ii. Máxima pérdida de datos tolerable / Objetivo punto de recuperación (RPO).
    iii. Tiempo de recuperación para empezar la operación de emergencia.

iv. Nivel de recuperación (capacidad relacionada con la operación regular).

v. Tiempo de restablecimiento hasta operación normal.

b) **Prestaciones**: medidas relativas a la capacidad de carga que el CSP deberá proporcionar.

c) **Consecuencias** de no cumplimiento.

d) **Disposiciones que limiten** los cambios implementados por el CSP que puedan impactar directamente en la infraestructura del CSC.

6.3.2 COPIAS DE SEGURIDAD (BCK)

24. Las copias de seguridad consistirán en imágenes de los sistemas/máquinas (*snapshots*) y/o copias de archivos que permitan recuperar datos de una antigüedad determinada conforme a la normativa aplicable. Estas copias abarcarán la información de la organización, aplicaciones, sistema operativo, datos de servicios y equipos, claves, etc., y tendrán el mismo nivel de seguridad que los datos originales.

6.4 DOMINIO 4 (D4): CONTROL DE CAMBIOS Y GESTIÓN DE CONFIGURACIÓN

25. Este dominio de seguridad incluye las medidas orientadas a que únicamente los cambios aprobados y en línea con los requisitos funcionales sean implementados y adecuadamente documentados.

6.4.1 GESTION DE LA CONFIGURACIÓN (GCF)

26. Abarca el proceso de gestión y mantenimiento de la configuración desplegada en el sistema y en los elementos que lo componen.

6.5 DOMINIO 5 (D5): CIFRADO, CRIPTOGRAFÍA Y GESTIÓN DE CLAVES

27. Este dominio de seguridad se refiere a la identificación de mecanismos apropiados de cifrado y gestión de claves con objeto de suministrar un acceso seguro a los recursos en la nube y la protección del dato.

6.5.1 PROTECCIÓN DE LAS COMUNICACIONES (PCM)

28. Esta medida recoge los requisitos de protección de las comunicaciones relativos a confidencialidad, integridad y autenticación extremo a extremo.

6.5.2 PROTECCIÓN DE SOPORTES (PSI)

29. Esta medida recoge los requisitos de protección criptológica de la información en los soportes de almacenamiento.

6.5.3 GESTIÓN DE CLAVES (GCK)

30. Abarca el proceso de generación, importación, actualización, sustitución, reemplazo, custodia y borrado de claves criptográficas utilizadas por los mecanismos criptográficos.

6.6 DOMINIO 6 (D6): SEGURIDAD EN EL CENTRO DE PROCESAMIENTO DE DATOS (CPD)

31. La seguridad en el centro de datos dependerá exclusivamente del CSP. El CPD deberá cumplir con todas las medidas de seguridad establecidas en la normativa aplicable según el tipo de información. El requisito ASI recoge todas las medidas relacionadas con la auditoría de seguridad del CPD, por lo que no se han incluido medidas adicionales.

6.7 DOMINIO 7 (D7): GESTIÓN DE LA PRIVACIDAD Y LA SEGURIDAD DEL DATO

32. Este dominio de seguridad se refiere a las medidas de seguridad orientadas a asegurar la adecuada identificación y control de los datos procesados, almacenados o intercambiados en la nube, así como el mantenimiento de la información en términos de custodia o propiedad, así como su confidencialidad, integridad y disponibilidad.

6.7.1 FIREWALL DE APLICACIÓN WEB (WAF)

33. Los *firewalls* de aplicación web protegen a los servidores de aplicaciones web de múltiples ataques. Para ello, monitorizan solicitudes HTTP/HTTPS y patrones de tráfico.

6.7.2 PREVENCIÓN DE FUGA DE DATOS (DLP)

34. Una solución DLP (*Data Loss Prevention*) está diseñada para detectar y prevenir brechas en la seguridad de la información sensible, monitorizando, detectando y bloqueando su utilización no autorizada, mientras se encuentra "en uso" (*endpoints*), "en movimiento" (tráfico de red) o "en reposo" (almacenamiento de datos), por medio de inspecciones profundas de contenido, análisis de la seguridad contextual de una transacción (atributos del originador, objetos de datos, medio, tiempos, destinos, etc...).

6.7.3 CASB (CASB)

35. Las herramientas CASB (*Cloud Access Security Broker*) gestionan las políticas de seguridad establecidas en la organización entre esta y el CSP. Este tipo de herramientas proporcionan al organismo que las utiliza visibilidad en el uso de las aplicaciones en la nube y el *shadow* IT, análisis de comportamiento de los usuarios,

control de accesos, cumplimiento de políticas y conformidad frente a estándares, etc…

6.7.4 BORRADO SEGURO (BSD)

36. Los mecanismos de borrado seguro permiten eliminar la información de manera que no sea recuperable.

6.8 DOMINIO 8 (D8): GOBERNANZA, RIESGO Y CUMPLIMIENTO

37. Este dominio de seguridad se define para ayudar a la organización a realizar una apropiada gobernanza de la seguridad y una gestión de riesgos adecuada a la hora de proporcionar servicios en la nube.
38. No se han definido medidas específicas adicionales para este dominio.

6.9 DOMINIO 9 (D9): RECURSOS HUMANOS

39. Este dominio de seguridad contempla todos los requisitos de validación de que los usuarios son confiables antes de permitir el acceso a los servicios en la nube, exigiendo habilitaciones de seguridad si fuera preciso.
40. Dado que el personal de administración tiene un control total sobre los sistemas, deberán considerarse específicamente los requisitos a cumplir por dicho personal, tanto para el CSP como para el CSC.
41. También incluye la definición de la estrategia de roles y permisos de usuario.

6.9.1 GESTION DE USUARIOS (GUS)

42. Esta medida recoge los requisitos mínimos que se requieren a los posibles usuarios/administradores del sistema en función de los privilegios de acceso que requieran, así como la estrategia de definición de permisos.

6.10 DOMINIO 10 (D10): GESTIÓN DE IDENTIDAD Y ACCESO

43. Este dominio de seguridad se refiere al conjunto de medidas requeridas para asegurar la identificación de usuarios dentro de los servicios en la nube con objeto de determinar un nivel de acceso apropiado a la información y los recursos.

6.10.1 CONTROL DE ACCESOS (CAC)

44. Esta medida define los criterios relativos a control de acceso a los recursos de los distintos usuarios del sistema.

6.10.2 IDENTIFICACIÓN Y AUTENTICACIÓN (I&A)

45. El proceso de identificación y autenticación de los usuarios se basa en el empleo de uno o varios de los siguientes factores, en función del nivel de seguridad requerido:

a) **Algo que se sabe**: Contraseñas o claves concertadas.

b) **Algo que se tiene**: Componentes lógicos, tales como certificados *software* o dispositivos físicos (*tokens*).

c) **Algo que se es**: elementos biométricos (lector de huella, iris, etc.).

46. Además, para el proceso de identificación y autenticación suele establecerse un número máximo de intentos de autenticación, de cara a evitar ataques de autenticación por fuerza bruta.

6.10.3 CONTROL DE SESIÓN (CSS)

47. Son las medidas dedicadas a controlar las sesiones de usuario, especialmente su duración, de tal forma que se pueda asegurar que se cierran de manera segura y no quedan sesiones abiertas que puedan suponer una amenaza para el servicio.

6.11 DOMINIO 11 (D11): INTEROPERABILIDAD Y PORTABILIDAD

48. Este dominio está orientado a garantizar la migración segura de las operaciones/servicios/datos desde la nube de un proveedor a otro preservando la interoperabilidad y disponibilidad. El objetivo de seguridad es evitar la dependencia de un fabricante/tecnología.

49. No se han definido medidas específicas adicionales para este dominio.

6.12 DOMINIO 12 (D12): INFRAESTRUCTURA Y VIRTUALIZACIÓN

50. Este control de seguridad contempla las medidas orientadas a mitigar los riesgos asociados al uso de una arquitectura *multi-tenant* y al aislamiento entre máquinas virtuales.

6.12.1 GESTIÓN DE INFRAESTRUCTURA (GIV)

51. La gestión de la infraestructura virtualizada comprende las actividades y los permisos de creación, configuración, mantenimiento y destrucción de máquinas virtuales.

6.12.2 AISLAMIENTO DE DATOS Y RECURSOS (ADR)

52. Son medidas orientadas a asegurar un completo aislamiento de los datos, tanto en reposo como en uso entre los diferentes sistemas VMs/host, incluyendo sus respectivos procesos y recursos tales como memorias o medios de almacenamiento. En particular, están enfocadas a limitar las funcionalidades que permiten la transferencia de datos entre máquinas virtuales o con el host.

6.12.3 SEPARACIÓN *HARDWARE* (SHW)

53. Tradicionalmente, los servicios en la nube se caracterizan por la compartición de recursos, tanto de almacenamiento como de procesamiento, entre los diferentes

consumidores del servicio o *tenants*. Bajo esta medida, se recogen todas las restricciones relativas a la compartición de recursos que, por cuestiones de seguridad, deban imponerse al sistema.

6.12.4 UBICACIÓN *HARDWARE* (UHW)

54. Esta medida contempla todas las restricciones relativas a la ubicación geográfica del *hardware* del sistema de información que da el servicio en la nube.

6.12.5 PROTECCIÓN DEL PERIMETRO (PDP)

55. Esta medida recoge los requisitos de protección perimetral. En ella se detallarán las funcionalidades de seguridad mínimas que debe implementar la capa de protección perimetral.

6.12.6 SEGREGACIÓN DE REDES (SGR)

56. Esta medida recoge los requisitos de segregación de las redes que dan el servicio al usuario frente a las redes utilizadas por otros usuarios.

6.13 DOMINIO 13 (D13): REGISTRO Y MONITORIZACIÓN

57. Este dominio de seguridad está dirigido a la recolección, la gestión y el ciclo de vida de los registros y las actividades de monitorización de los entornos en la nube.

6.13.1 GESTIÓN DE EVENTOS (GES)

58. Son mecanismos que permiten el almacenamiento y retención de logs y eventos de seguridad generados por el sistema y/o los usuarios durante un periodo de tiempo determinado, conforme a la política aplicable la organización.
59. Además, pueden implementarse mecanismos de correlación de eventos que los complementen y que facilitan la búsqueda de anomalías o posibles amenazas para la seguridad del sistema.

6.14 DOMINIO 14 (D14): GESTIÓN DE INCIDENTES DE SEGURIDAD, *E-DISCOVERY* Y FORENSE EN LA NUBE

60. Este dominio de seguridad abarca todas las medidas de seguridad requeridas para asegurar la detección, respuesta, notificación y remediación efectiva de incidentes. Incluye medidas específicas de seguridad en apoyo al descubrimiento de datos sensibles y el análisis forense.
61. No se han definido medidas específicas adicionales para este dominio.

6.15 DOMINIO 15 (D15): GESTIÓN DE LA CADENA DE SUMINISTRO, TRANSPARENCIA Y RESPONSABILIDAD

62. Este dominio de seguridad abarca las medidas orientadas a conseguir una adecuada verificación de los estándares de calidad y seguridad asociados a los procesos de negocio y producción del proveedor.

63. No se han definido medidas específicas adicionales para este dominio.

6.16 DOMINIO 16 (D16): GESTIÓN DE VULNERABILIDADES Y AMENAZAS

64. Este dominio de seguridad se refiere al desarrollo de procedimientos e implementación de medidas técnicas para identificar amenazas, detectar vulnerabilidades y prevenir su explotación.

6.16.1 GESTIÓN DE ACTUALIZACIONES (GAC)

65. Abarca el proceso de gestión de las actualizaciones publicadas por los fabricantes de productos, principalmente de aquellas relacionadas con la seguridad y la remediación de vulnerabilidades en los sistemas y sus componentes.

6.17 DOMINIO 17 (D17): GESTIÓN DEL *ENDPOINT*

66. Este dominio de seguridad define las medidas de seguridad a implementar en la configuración y gestión de los *endpoints* que vayan a conectarse a la infraestructura en la nube.

6.17.1 GESTIÓN DEL ENDPOINT (GEP)

67. En esta medida se recogerán todas las medidas de bastionado del *endpoint* desde el que el usuario accede al servicio en la nube. Para ello, se tomará como referencia la arquitectura descrita en la guía *CCN-STIC-498 Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro)* [3].

7. ANÁLISIS DE ARQUITECTURAS

68. Teniendo en cuenta las distintas categorías de servicio y el grado de clasificación de la información que se va a manejar en la nube, se describen las siguientes arquitecturas:

	IAAS	PAAS	SAAS
SIN CLASIFICAR	Arquitectura 1.1	Por definir	Por definir
DIFUSIÓN LIMITADA	Arquitectura 1.2	Por definir	Por definir
CONFIDENCIAL O SUPERIOR	Arquitectura 1.3	Por definir	Por definir

69. En cuanto a los modelos de despliegue, por simplicidad, se excluyen del análisis del presente documento las arquitecturas para nube híbrida, dado que se trata de arquitecturas con partes en nube pública y partes en privada que deberán analizarse individualmente.

70. Por defecto, se aplicará el principio de seguridad en todas las capas.

7.1 ARQUITECTURAS IAAS

71. Como ya se indicó la Sección 4.2, en este caso la configuración, operación y mantenimiento de la capa de infraestructura son responsabilidad del CSP, mientras que la plataforma y servicios que corren sobre ella son responsabilidad del CSC.

7.1.1 MEDIDAS DE SEGURIDAD PARA ARQUITECTURA IAAS

72. La siguiente tabla presenta un resumen de las medidas que debe implementar el Sistema dependiendo del nivel de clasificación de la información que va a manejar. En ella se diferencian diferentes niveles de seguridad incrementales L1, L2 y L3 y si estas aplican al CSC, al CSP o a ambos.

		IAAS		
		SIN CLASIFICAR	**DIFUSIÓN LIMITADA**	**CONF O SUPERIOR**
(D1): Auditoría y aseguramiento				
Auditoría del Sistema de Información (ASI)	CSP	L1	L2	L3
	CSC	L1	L2	L3

		IAAS		
		SIN CLASIFICAR	DIFUSIÓN LIMITADA	CONF O SUPERIOR
Sometimiento jurisdiccional (SJD)	CSP	L1	L2	L2
	CSC	L1	L2	L2
(D2): Seguridad de aplicaciones e interfaces				
Cualificación de servicio en la nube (CSN)	CSP	L1	--	--
	CSC	L1	--	--
Cualificación de producto (CPN)	CSP	--	--	--
	CSC	L1	--	--
Aprobación de servicio en la nube (ASN)	CSP	--	L1	L2
	CSC	--	L1	L2
Aprobación de producto (APN)	CSP	--	L1	L2
	CSC	--	L1	L2
(D3): Gestión de continuidad de negocio y resiliencia de operaciones				
Acuerdo a nivel de servicio (SLA)	CSP	L1	L1	L1
	CSC	--	--	--
Copias de seguridad (BCK)	CSP	--	--	--
	CSC	L1	L2	L2
(D4): Control de cambios y gestión de configuración				
Gestión de la configuración (GCF)	CSP	--	--	--
	CSC	L1	L2	L2
(D5): Cifrado, criptografía y gestión de claves				
Protección de las comunicaciones (PCM)	CSP	L1	L1	L1
	CSC	L1	L2	L3
Protección de soportes de información (PSI)	CSP	--	--	--
	CSC	L1	L2	L3
Gestión de claves (GCK)	CSP	--	--	--
	CSC	L1	L2	L2

		IAAS		
		SIN CLASIFICAR	DIFUSIÓN LIMITADA	CONF O SUPERIOR
(D7): Gestión de la seguridad del dato y privacidad				
Firewall de aplicación web (WAF)	CSP	--	--	--
	CSC	L1	L2	L3
Prevención de fuga de datos (DLP)	CSP	--	--	--
	CSC	L1	L1	L1
CASB (CASB)	CSP	--	--	--
	CSC	L1	L1	L1
Borrado seguro de datos (BSD)	CSP	L1	L2	L2
	CSC	L1	L2	L2
(D9): Recursos humanos				
Gestión de Usuarios (GUS)	CSP	--	L2	L2
	CSC	L1	L2	L2
(D10): Gestión de identidad y acceso				
Control de accesos (CAC)	CSP	--	--	--
	CSC	L1	L1	L1
Identificación y Autenticación (I&A)	CSP	--	--	--
	CSC	L1	L1	L1
Control de sesión (CSS)	CSP	--	--	--
	CSC	L1	L2	L2
(D12): Infraestructura y virtualización				
Gestión de infraestructura virtualizada (GIV)	CSP	L1	L1	L1
	CSC	L1	L1	L1
Aislamiento de datos y recursos (ADR)	CSP	--	--	--
	CSC	--	L1	L2
Separación *hardware* (SHW)	CSP	-	L1	L2
	CSC	--	--	--

		IAAS		
		SIN CLASIFICAR	DIFUSIÓN LIMITADA	CONF O SUPERIOR
Ubicación *hardware* (UHW)	CSP	L1	L2	L2
	CSC	--	--	--
Protección del perímetro (PDP)	CSP	L1	L2	L2
	CSC	L1	L2	L3
Segregación de redes (SGR)	CSP	--	--	--
	CSC	L1	L2	L2
(D13): Registro y monitorización				
Gestión de eventos (GES)	CSP	--	--	--
	CSC	L1	L1	L1
(D16): Gestión de vulnerabilidades y amenazas				
Gestión de actualizaciones (GAC)	CSP	--	--	--
	CSC	L1	L1	L1
(D17): Gestión del *EndPoint*				
Gestión del *EndPoint* (GEP)	CSP	--	--	--
	CSC	L1	L2	L3

7.1.2 ARQUITECTURA 1.1: IaaS PARA MANEJAR INFORMACIÓN SIN CLASIFICAR

73. En el siguiente esquema se presenta un resumen de las medidas asociadas a cada uno de los actores que es necesario implementar en esta arquitectura.

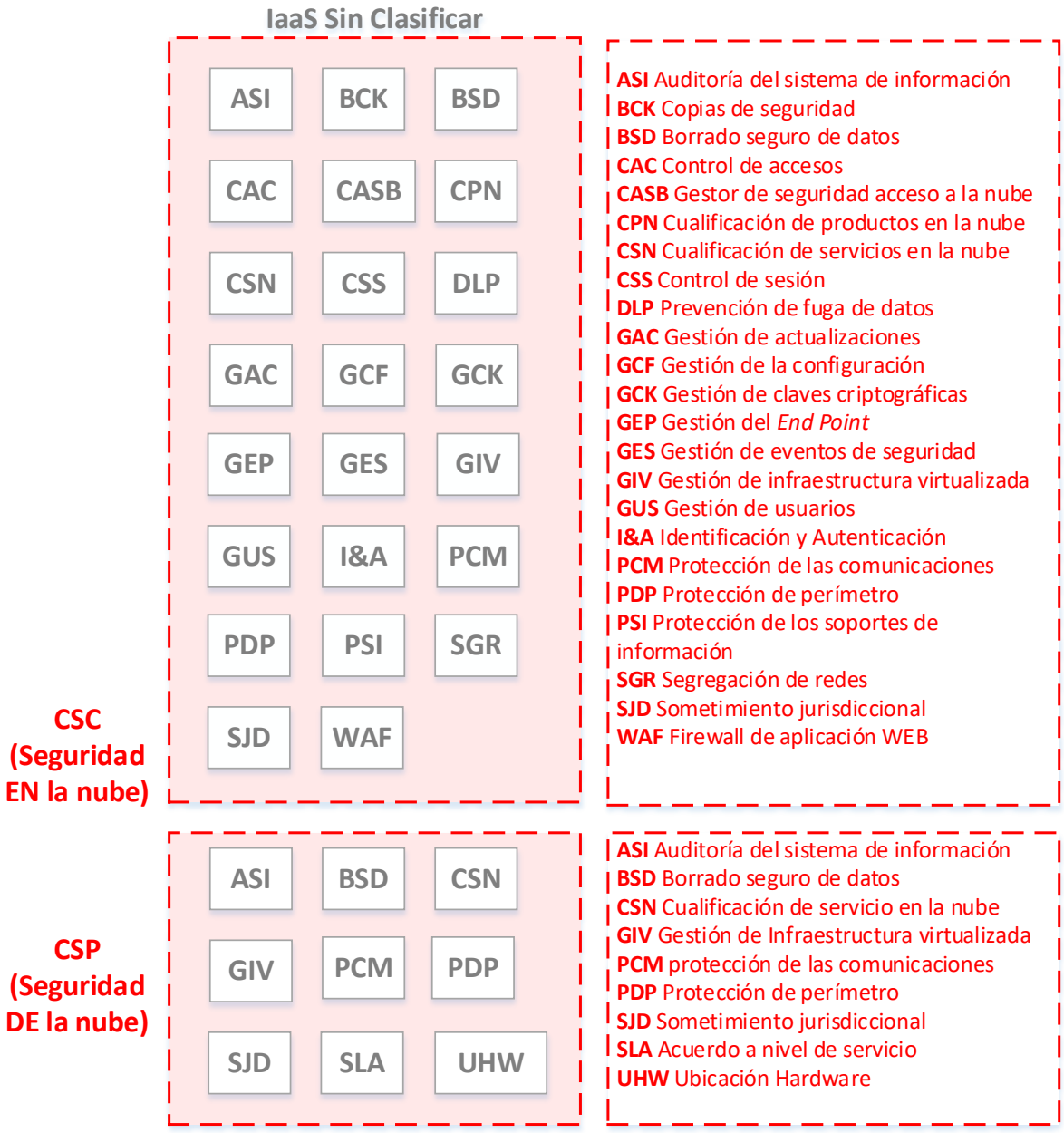


Figura 2. Medidas de Seguridad IaaS en nube sin clasificar

74. Partiendo de las medidas de seguridad descritas en la Sección 6, se incluye una descripción del subconjunto de estas que deben considerarse para implementar una arquitectura segura para el escenario en el que el/los sistemas manejen únicamente información SIN CLASIFICAR.

75. En el ANEXO A se incluye un diagrama detallado de alto nivel que cubre las medidas de seguridad que se definen en la siguiente sección.

7.1.2.1 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSP

7.1.2.1.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L1

76. Todos los sistemas que manejen información no clasificada serán objeto de **auditorías de seguridad, según la normativa de aplicación**. Por ejemplo, para sistemas bajo el alcance del Esquema Nacional de Seguridad, se deberá realizar una auditoría de conformidad que garantice el cumplimiento de los requisitos determinados por la Declaración de Aplicabilidad. En dicha auditoría se evaluarán los requisios que son responsabilidad del CSP.

7.1.2.1.2 D1: SOMETIMIENTO JURISDICCIONAL (SJD) – L1

77. Todos los sistemas que manejen información sensible no clasificada, por ejemplo, para sistemas bajo el alcance del Esquema Nacional de Seguridad o sistemas que manejen información de USO OFICIAL, deberán estar sometidos exclusivamente a la jurisdicción española.

7.1.2.1.3 D2: CUALIFICACIÓN DE SERVICIO EN LA NUBE (CSN) - L1

78. Los servicios de seguridad ofrecidos por el CSP deberán estar cualificados e incluidos en el listado de **Servicios Cualificados del CPSTIC**. Si en el momento de la contratación no existiesen servicios en el listado de Servicios Cualificados se utilizarán, preferiblemente, servicios que cuenten con una certificación de seguridad reconocida por el Organismo de Certificación del ENECSTI.

7.1.2.1.4 D3: ACUERDO DE SERVICIO (SLA) - L1

79. El CSC y el CSP deberán firmar un SLA donde se establezcan los **requisitos mínimos** indicados en la Sección 6. Será responsabilidad del CSP implementar todos mecanismos para garantizar el cumplimiento de los compromisos adquiridos y realizar **pruebas periódicas** para evaluar el correcto funcionamiento de los mismos.
80. El CSC deberá realizar un análisis para determinar cuáles son los umbrales adecuados para satisfacer sus **necesidades de continuidad y disponibilidad y exigirlos** al CSP, a través del SLA.

7.1.2.1.5 D5: PROTECCIÓN DE LAS COMUNICACIONES (PCM) - L1

81. Deberán aplicarse mecanismos criptográficos para la protección de la confidencialidad e integridad de la información en tránsito mediante la utilización de **redes privadas virtuales (VPN) que hayan superado con éxito un proceso de cualificación**. En este caso, el canal de comunicación aportará también autenticación extremo a extremo. La utilización de cifrado *on line* será obligatoria siempre que se envíe información fuera del sistema que provee la infraestructura.
82. La configuración de dichas VPN deberá utilizar algoritmos, protocolos y mecanismos criptográficos autorizados por el CCN en la guía **CCN-STIC-807** [4].

83. Todo el tráfico entrante y saliente pasará por la VPN y no existirá ningún tráfico fuera de ella que pueda suponer un canal encubierto.
84. Todas las claves criptográficas que se encuentren en uso deberán **almacenarse de manera segura**, utilizando mecanismos que presenten, al menos, la misma fortaleza que la de las claves.
85. La protección de las comunicaciones será aplicable, tanto a las comunicaciones con entidades externas, como a las establecidas dentro de la infraestructura en la nube, cuando se transmita por medios compartidos.

7.1.2.1.6 D7: BORRADO SEGURO DE DATOS (BSD) - L1

86. Se implementarán mecanismos de borrado seguro que permitan al usuario eliminar la información de manera que no sea recuperable una vez que finalice su uso.

7.1.2.1.7 D12: GESTIÓN DE INFRAESTRUCTURA VIRTUALIZADA (GIV) - L1

87. La gestión de la infraestructura virtualizada permitirá desplegar y configurar aplicaciones e infraestructuras tales que los accesos de los usuarios (*tenant*) e *intratenant* estén apropiadamente segregados y segmentados. Para ello, deberán tenerse en cuenta los siguientes puntos:
    a) Definición de zonas de seguridad que deben estar separadas.
    b) En qué casos los CSC deben estar (criptológica, lógica o físicamente) segregados.
    c) Qué relaciones de comunicación y qué redes y protocolos de aplicación están permitidos en cada caso.
    d) Cómo el tráfico de datos para administración y monitorización está segregado en cada nivel de red.
    e) Qué comunicaciones internas o entre distintas redes están permitidas.
88. En todos los puntos indicados anteriormente, se deberá utilizar el principio de denegación total por defecto.
89. En base a lo anterior, se implementarán medidas de bastionado para los componentes del Sistema, *hosts* y sistemas operativos, hipervisores o control de infraestructura, acorde a las mejores prácticas de cada fabricante y a los Procedimientos de Empleo Seguro, en caso de productos cualificados/aprobados. Deberán además existir controles técnicos de verificación de la configuración como parte de la base de seguridad.
90. Además, deberán segregarse entornos de producción y no producción.

7.1.2.1.8 D12: UBICACIÓN *HARDWARE* (UHW) – L1

91. Todos los datos de usuario y logs generados por este que contengan información personal deberán cumplir lo dispuesto en el Reglamento General de Protección de Datos [5].

92. En todo caso, el CSP estará obligado a entregar al CSC información relativa a la ubicación geográfica de almacenamiento y procesamiento de su información, copias de *backup* y registros de *logs*.

7.1.2.1.9 D12: PROTECCIÓN DEL PERIMETRO (PDP) – L1

93. Dado que se aplica el principio de seguridad en todas las capas, el CSC será el responsable de establecer las protecciones perimetrales necesarias para proteger los servicios que corren sobre la infraestructura contratada, mientras que el CSP será el responsable de implementar las medidas de protección perimetral para el servicio que ofrece, como un elemento más de lo que se ha denominado "seguridad DE la nube".

7.1.2.2 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSC

7.1.2.2.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L1

94. Todos los sistemas que manejen información no clasificada serán objeto de **auditorías de seguridad, según la normativa de aplicación**. Por ejemplo, para sistemas bajo el alcance del Esquema Nacional de Seguridad, se deberá realizar una auditoría de conformidad que garantice el cumplimiento de los requisitos determinados por la Declaración de Aplicabilidad. En dicha auditoría se evaluarán los requisios que son responsabilidad del CSC.

7.1.2.2.2 D1: SOMETIMIENTO JURISDICCIONAL (SJD) – L1

95. Todos los sistemas que manejen información sensible no clasificada, por ejemplo, para sistemas bajo el alcance del Esquema Nacional de Seguridad o sistemas que manejen información de USO OFICIAL, deberán estar sometidos exclusivamente a la jurisdicción española.

7.1.2.2.3 D2: CUALIFICACIÓN DE SERVICIO EN LA NUBE (CSN) Y CUALIFICACIÓN DE PRODUCTO (CPN) – L1

96. Siempre que sea posible, en la arquitectura de seguridad del Sistema se utilizarán **productos o servicios** que hayan sido incluidos en el apartado Cualificados del **CPSTIC**.

7.1.2.2.4 D3: COPIAS DE SEGURIDAD (BCK) –L1

97. Con carácter general, se recomienda realizar **regularmente copias de seguridad** mediante imágenes (*snapshots*) o copias de archivos que permitan recuperar datos

de una antigüedad determinada conforme a la política de seguridad de la organización. Estas copias podrán abarcar la información, los logs del Sistema, las aplicaciones, los sistemas operativos, claves, etc., y exigirán el mismo nivel de seguridad que los datos originales.

98. Cuando las copias puedan ser ejecutadas y transferidas remotamente, se establecerán **canales seguros**, para los que se utilizarán herramientas cualificadas.

99. Dado que se no se trata de información clasificada, este servicio podría encontrarse entre los ofrecidos por el propio CSP y contemplado en los acuerdos recogidos dentro del SLA, o ser gestionado por el propio cliente.

100. El proceso de restauración de dichas copias debe estar sujeto a un **programa de pruebas periódicas** que verifiquen su correcto funcionamiento**.** Estas pruebas se realizarán **al menos una vez al año** y en ellas, deberá comprobarse:

a) El alcance y la frecuencia de los *backups* de datos. Se monitorizará su realización.

b) La duración de la retención es consistente con los acuerdos contractuales establecidos en el SLA relativos a *Recovery Time Objetive* (RTO) *y Recovery Point Objetive (RPO).*

c) El acceso a los datos de *backup* y la restauración se realiza únicamente por personas autorizadas.

7.1.2.2.5 D4: GESTION DE LA CONFIGURACIÓN (GCF) – L1

101. Las configuraciones *software* de los componentes que se suben a la nube deberán estar autorizadas por la Política de Seguridad de la organización, a nivel de servidores, estaciones de trabajo o elementos de red virtualizados. Dicha configuración debe ser **analizada con una periodicidad establecida** para verificar que no existen deficiencias que puedan constituir un riesgo para el Sistema.

102. Dicha gestión de la configuración puede ser realizada manualmente, a través de herramientas autorizadas que el CSC sube a la nube o haciendo uso de servicios de gestión de la configuración suministrados por el CSP.

7.1.2.2.6 D5: PROTECCIÓN DE LAS COMUNICACIONES (PCM) – L1

103. Deberán aplicarse mecanismos criptográficos para la protección de la confidencialidad e integridad de la información en tránsito mediante la utilización de **redes privadas virtuales (VPN)**. En este caso, el canal de comunicación aportará también autenticación extremo a extremo. La utilización de cifrado *on line* será obligatoria siempre que se envíe información fuera del Sistema gestionado por el usuario o entre cada una de los distintos subsistemas que lo componen.

104. Todos los productos o servicios de cifrado *on line* deberán estar incluidos en el apartado de productos o servicios cualificados del CPSTIC y se configurarán de tal manera que utilicen algoritmos, protocolos y mecanismos criptográficos autorizados por el CCN en la guía **CCN-STIC-807** [4].

105. Todas las claves criptográficas que se encuentren en uso deberán **almacenarse de manera segura**, utilizando mecanismos que presenten, al menos, la misma fortaleza que la de las claves.

7.1.2.2.7 D5: PROTECCIÓN DE SOPORTES (PSI) – L1

106. Deberá implementarse protección de la confidencialidad e integridad de la información almacenada mediante mecanismos de cifrado en reposo (*at-rest*).

107. Todos los productos o servicios de cifrado en reposo deberán estar incluidos en el apartado de **productos o servicios cualificados del CPSTIC** y se configurarán de tal manera que utilicen algoritmos, protocolos y mecanismos criptográficos autorizados por el CCN en la guía **CCN-STIC-807** [4].

7.1.2.2.8 D5: GESTIÓN DE CLAVES (GCK) – L1

108. Para la gestión de claves criptográficas se utilizarán **herramientas cualificadas** de gestión de claves (*KMS, Key Management System*) o servicios cualificados de gestión de claves basados en HSM. Preferiblemente, se utilizarán claves generadas por el usuario que se reemplazarán periódicamente de acuerdo a la política establecida.

109. Todas las claves criptográficas que se encuentren en uso **deberán almacenarse de manera segura**, utilizando mecanismos que presenten, al menos, la misma fortaleza que la de las claves.

7.1.2.2.9 D7: FIREWALL DE APLICACIÓN WEB (WAF) - L1

110. El CSC será el responsable del despliegue de un *firewall* de aplicación web para proteger sus recursos, que debe haber **superado con éxito un proceso de cualificación.**

111. Todo el tráfico de acceso a los recursos desde Internet deberá ser enrutado a través de este WAF, que detectará y bloqueará tráfico entrante que pudiera suponer una amenaza para el servicio web.

7.1.2.2.10 D7: PREVENCIÓN DE FUGA DE DATOS/CASB (DLP/CASB) – L1

112. Deberán utilizarse mecanismos que permitan controlar la información exportada desde el Sistema y habilitar únicamente los medios externos autorizados. Aunque el control de dicha información puede realizarse mediante medidas no automatizadas, la utilización de dispositivos DLP cualificados está recomendada.

7.1.2.2.11 D7: BORRADO SEGURO DE DATOS (BSD) - L1

113. Se implementarán mecanismos de borrado seguro que permitan al usuario eliminar la informaciónde manera que no sea recuperable una vez que finalice su uso.

114. Las herramientas utilizadas para el borrado debeberán estar incluidas en el listado de Productos Cualificados del CPSTIC.

7.1.2.2.12 D9: GESTION DE USUARIOS (GUS) – L1

115. Para un mismo sistema, deberán establecerse diferentes usuarios con diferentes niveles de privilegios, de forma que:

    a) Únicamente se podrá administrar el Sistema desde un perfil de administrador.

    b) Las sesiones de administración únicamente se emplearán para administrar el Sistema.

    Se implementará una configuración que limite y controle la ejecución de *software* de acuerdo con los principios de mínima funcionalidad y mínimo privilegio.

7.1.2.2.13 D10: CONTROL DE ACCESOS (CAC) – L1

116. El control de acceso de los usuarios a los recursos y datos del Sistema se hará en base a la existencia de diferentes perfiles. Como mínimo, se definirán dos (2) tipos de perfiles: el no privilegiado y el privilegiado. Entre los usuarios privilegiados podrían estar los administadores de seguridad, auditores del Sistema, etc.

117. El control de accesos deberá permitir aplicar los siguientes criterios:

    a) Todo acceso debe estar prohibido, salvo concesión expresa.

    b) Los privilegios de cada entidad, usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).

    c) Cada entidad quedará identificada singularmente.

    d) La utilización de los recursos debe estar protegida.

    e) La identidad de la entidad deberá quedar previamente autenticada.

    f) Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos.

7.1.2.2.14 D10: IDENTIFICACIÓN Y AUTENTICACIÓN (I&A) – L1

118. Se requerirá que el usuario haya superado un proceso de identificación positiva antes de realizar cualquier acción sobre el Sistema.

119. Preferentemente, se utilizará un doble factor de autenticación para la autenticación de los usuarios, aunque podrá basarse en el empleo de un único factor mediante usuario y contraseña siempre y cuando se cumplan los requisitos especificados a continuación:

    - Las contraseñas deberán ser gestionadas siguiendo los procedimientos de seguridad establecidos por la organización, que deberán especificar:
        - La periodicidad con la que se actualizan.

- El número de contraseñas anteriormente utilizadas que no debe repetirse. No se permirá la repetición de, al menos, las 10 últimas contraseñas utilizadas y no se podrá realizar un nuevo cambio de contraseña, como mínimo, en los 4 días posteriores al último cambio.
- La longitud mínima y características de las contraseñas. Esta longitud mínima deberá ser mayor o igual a 12 caracteres e incluir, al menos, un carácter de los siguientes grupos: caracteres especiales, mayúsculas, minúsculas y números.
- Se indicará que las contraseña deberán modificarse la primera vez que se inicie la sesión.

- Se fijará un tiempo máximo de validez de contraseñas de 30 días.

120. Se forzará una renovación de todas las credenciales cuando estas hayan sido comprometidas.

121. El servicio bloqueará el acceso y requerirá un nuevo proceso de identificación y autenticación en los siguientes casos:

a) Después de un determinado período de inactividad o cuando el propio usuario bloquee la sesión. En este caso, se bloqueará la sesión activa y se impedirá cualquier acción sobre el Sistema a menos que un usuario la desbloquee.

b) Después de varios intentos fallidos de acceso. En este caso, se impedirá cualquier acción sobre el servicio hasta que un administrador autorizado la desbloquee o se establezca un procedimiento alternativo de desbloqueo que deberá ser autorizado caso por caso.

7.1.2.2.15 D10: CONTROL DE SESIÓN (CSS) – L1

122. Se informará al usuario del último acceso efectuado con su identidad.

123. El Sistema se configurará de tal forma que se establezca un tiempo máximo de inactividad de sesión, a partir del cual, esta se cerrará.

7.1.2.2.16 D12: GESTIÓN DE INFRAESTRUCTURA (GIV) – L1

124. La funcionalidad de creación de máquinas virtuales deberá configurarse y controlarse adecuadamente. Esta funcionalidad estará restringida a usuarios privilegiados (administradores). Al finalizar su uso, las máquinas virtuales deberán tratarse del mismo modo que las físicas.

125. Toda la administración relacionada con la arquitectura de virtualización deberá realizarse de manera independiente para cada uno de los sistemas que residan en ella. El personal administrador de virtualización deberá realizar una administración aislada y específica para cada uno de ellos.

126. En el caso de máquinas virtuales que manejen información no clasificada, estas deberán permitir reiniciar su configuración cada vez que se produzca un arranque y mantener los registros de auditoría generados.

7.1.2.2.17 D12: PROTECCIÓN DEL PERIMETRO (PDP) – L1

127. Siempre que la infraestructura en la nube gestionada por el CSC se interconecte con otros sistemas, deberán utilizarse los dispositivos de protección de perímetro requeridos en la CCN-STIC-302 [6] para el grado de clasificación establecido. En el caso de información SIN CLASIFICAR deberá utilizarse, como mínimo, un *firewall*.

128. Estos dispositivos / servicios de protección de perímetro deberán figurar entre los productos / servicios cualificados del CPSTIC.

7.1.2.2.18 D12: SEGREGACIÓN DE REDES (SGR) – L1

129. Se utilizarán nubes privadas virtuales, configuradas por el CSC para incrementar el nivel de aislamiento ofrecido por el CSP entre los sistemas de los diferentes *tenats*. Estas VPC consisten en un conjunto de medidas basadas en la utilización de distintas subredes, así como en el establecimiento de canales seguros para cada *tenant*. De esta forma, se establecen nubes virtuales privadas mediante *software* que simulan una infraestructura dedicada para cada usuario.

7.1.2.2.19 D13: GESTION DE EVENTOS (GES) – L1

130. El Sistema deberá disponer de una referencia de tiempo (*timestamp*) confiable y autenticada para garantizar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del Sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

131. Se utilizarán mecanismos para el almacenamientode *logs* y eventos de seguridad generados por el Sistema y/o los usuarios, que permitan retener los registros durante el periodo que aplique conforme a la política establecida en la organización.

132. Los *logs* de sistemas operativos e hipervisores deberán contener, al menos:

    a) Eventos de autenticación de usuarios y administradores.

    b) Eventos de acciones realizadas sobre ficheros y objetos.

    c) Eventos de exportación (*upload*) e importación (*download*).

    d) Eventos de acciones sobre cuentas de usuarios.

    e) Eventos de acciones realizadas por usuarios privilegiados.

    f) Todos aquellos eventos adicionales reflejados en las diferentes políticas de seguridad de los sistemas.

7.1.2.2.20 D16: GESTIÓN DE ACTUALIZACIONES (GAC) – L1

133. Los sistemas deberán mantenerse convenientemente actualizados para protegerse frente a las nuevas amenazas o vulnerabilidades conocidas. Para los niveles de clasificación para los cuales no sea viable instalar de forma automática

actualizaciones de *software* o descarga de firmas, será necesario contemplar mecanismos manuales *offline*.

7.1.2.2.21 D17: GESTIÓN DEL ENDPOINT (GEP)

134. Se implementarán las medidas de bastionado descritas en la guía *CCN-STIC-498 Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro)* [3] para sistemas sin clasificar.

7.1.3 ARQUITECTURA 1.2: IaaS PARA MANEJAR INFORMACIÓN DIFUSIÓN LIMITADA

135. En esta sección, se definen las medidas de una arquitectura IaaS para manejar **información clasificada DIFUSIÓN LIMITADA** (DL) en la nube. Es imporante destacar que, en caso de que el sistema maneje información de mayor clasificación deberán aplicarse las medidas correspondientes al máximo nivel.
136. Además,, para el manejo de información clasificada cifrada con herramientas aprobadas, podrá implementarse la arquitectura descrita en el apartado anterior, ya que la información cifrada bajo las condiciones descritas no se considera información clasificada.
137. En el siguiente esquema se presenta un resumen de las medidas que es necesario implementar para esta arquitectura.

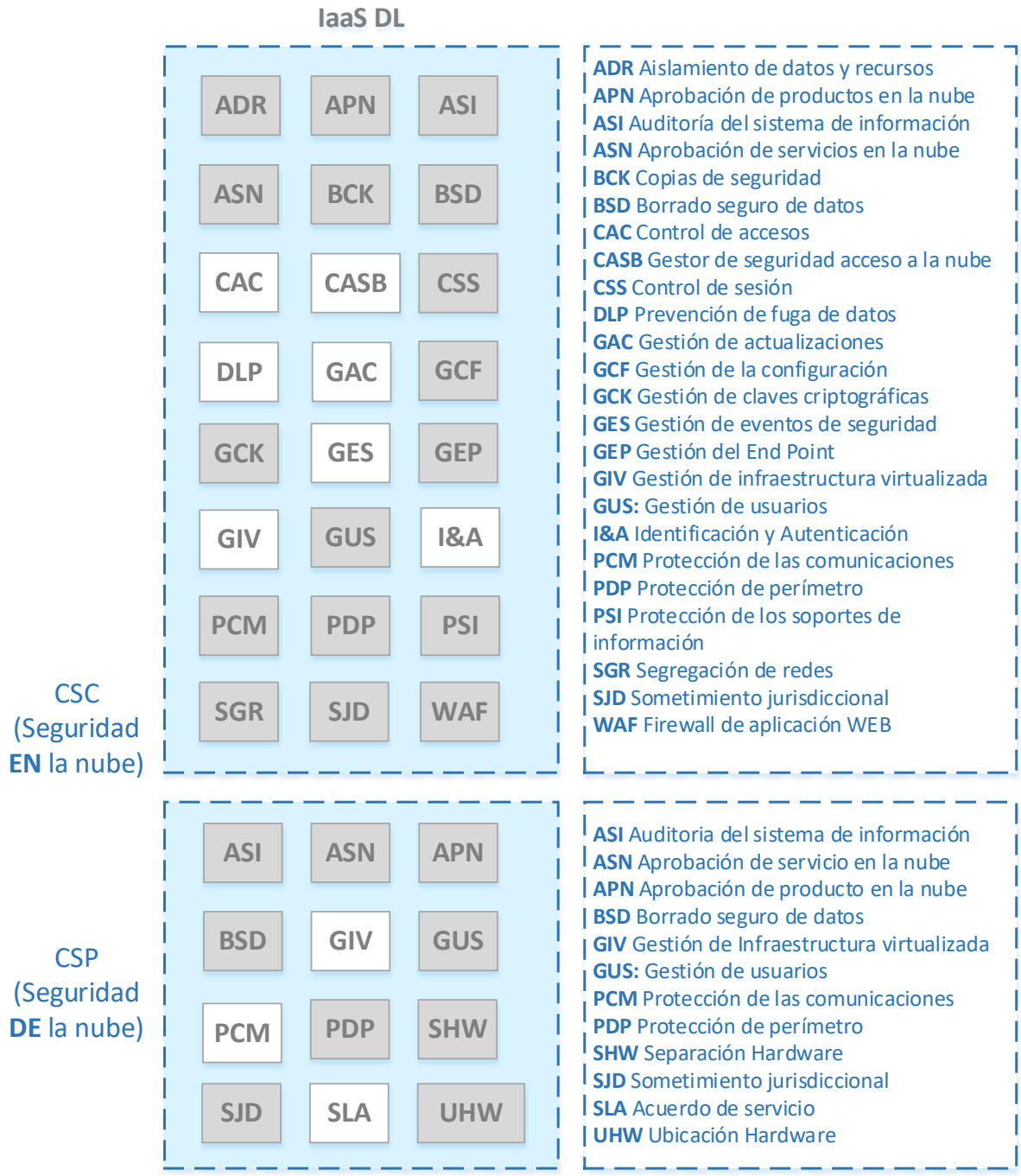


Figura 3. Medidas de Seguridad IaaS en nube pública Difusión Limitada

138. **Se han resaltado en gris aquellas medidas nuevas o que han sufrido modificaciones con respecto a la arquitectura de nube sin clasificar descrita en la Sección 7.1 (medidas nivel L2). Estas medidas se describen a continuación. El resto de medidas permanecen invariables y será aplicable lo descrito anteriormente.**

139. Para implementar una arquitectura segura para el escenario en el que el/los sistemas manejen información clasificada DIFUSIÓN LIMITADA en la nube**,** se aplicarán **todas las medidas del modelo de arquitectura descrita en la sección anterior y los elementos adicionales definidos a continuación**.

140. Es importante destacar que el listado de medidas de seguridad establecido en el presente documento cumple con la guía *CCN-STIC-301 Medidas de Seguridad TIC a implementar en sistemas clasificados* [7] y **parte de un escenario de uso genérico, que podrá ser modificado o refinado por los resultados del preceptivo análisis de riesgos para cada escenario de uso concreto**.

141. En el ANEXO B se incluye un diagrama detallado que, a alto nivel, cubre las medidas de seguridad que se definen en la siguiente sección.

7.1.3.1 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSP

7.1.3.1.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L2

142. Todos los sistemas que manejen información DIFUSIÓN LIMITADA **deberán estar acreditados por la Autoridad de Acreditación Nacional de acuerdo con la guía *CCN-STIC-001 Política de Seguridad de las TIC*** [8]**.**

7.1.3.1.2 D1: SOMETIMIENTO JURISFICCIONAL (SJD) – L2

143. Todos los sistemas que manejen información clasificada nacional, deberán estar sometidos exclusivamente a la jurisdicción española.

144. En el caso de sistemas que manejen **exclusivamente** información clasificada de otros ámbitos deberán cumplirse las restricciones de sometimiento jurisdiccional impuestas por la normativa que sea de aplicación.

7.1.3.1.3 D2: APROBACIÓN (ASN Y APN) – L1

145. Los servicios de seguridad ofrecidos por el CSP deberán estar **aprobados para manejar información DIFUSIÓN LIMITADA** e incluidos en el listado de Servicios Aprobados del **CPSTIC**.

7.1.3.1.4 D7: BORRADO SEGURO DE DATOS (BSD) – L2

146. Se implementarán mecanismos de borrado seguro que permitan al usuario eliminar la información de manera que no sea recuperable una vez que finalice su uso.

147. Para la sanitización de soportes que manejan información clasificada deberá cumplirse con lo establecido en la guía ***CCN-STIC-305 Destrucción y Sanitización de soportes informáticos*** [9] para el grado de clasificación del Sistema que se desee sanitizar.

7.1.3.1.5 D9: GESTIÓN DE USUARIOS (GUS) – L2

148. Para la gestión de usuarios será aplicable:

    a) Los sistemas o equipos desde el que un usuario administrador administra el servicio deberá estar acreditado al mismo nivel de clasificación.

    b) Se exigirá que todas las personas del CSP con privilegios de acceso al sistema como administrador dispongan de HPS expedida por la ANS con nivel igual o superior al de la información que vaya a manejar el sistema.

7.1.3.1.6 D12: SEPARACIÓN *HARDWARE* (SHW) – L1

149. Cuando se vaya a manejar información DL, se podrá compartir *hardware* en aquellos casos en los que exista una **autorización expresa de la Autoridad de Acreditación** correspondiente.

150. En general, se podrá compartir *hardware* entre sistemas DIFUSIÓN LIMITADA o sin clasificar, pertenecientes a un mismo organismo (**nube privada**) o a diferentes organismos que pertenezcan a una comunidad autorizada, cuyos miembros se determinarán mediante acuerdos cuando se establezca la arquitectura de nube (**nube comunitaria**).

7.1.3.1.7 D12: UBICACIÓN *HARDWARE* (UHW) – L2

151. El CSC deberá exigir al CSP información relativa a la ubicación geográfica de su información (datos, *logs, backups*, etc…) que, en todo caso, deberán estar ubicados en sistemas acreditados por la autoridad nacional correspondiente.

7.1.3.1.8 D12: PROTECCIÓN DEL PERIMETRO (PDP) – L2

152. Dado que se aplica el principio de seguridad en todas las capas, el CSC será el responsable de establecer las protecciones perimetrales necesarias para proteger los servicios que corren sobre la infraestructura contratada, mientras que el CSP será el responsable de implementar las medidas de protección perimetral para el servicio que ofrece, como un elemento más de lo que hemos denominado "**seguridad DE la nube**".

153. Como mínimo, deberán implementarse medidas de prevención frente a ataques que pudieran comprometer el servicio ofrecido al CSC.

7.1.3.2 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSC

7.1.3.2.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L2

154. Todos los sistemas que manejen información DIFUSIÓN LIMITADA deberán estar acreditados por la Autoridad de Acreditación Nacional de acuerdo con la guía *CCN-STIC-001 Política de Seguridad de las TIC* [8].D2: APROBACIÓN DE SERVICIO EN LA NUBE Y APROBACIÓN DE PRODUCTO EN LA NUBE (ASN Y APN) – L2

155. Siempre que sea posible, en la arquitectura de seguridad del Sistema se utilizarán **productos o servicios** que hayan sido incluidos como productos o servicios **aprobados en el CPSTIC** para el grado de clasificación **DIFUSIÓN LIMITADA**.

7.1.3.2.2 D1: SOMETIMIENTO JURISDICCIONAL (SJD) – L2

156. Todos los sistemas que manejen información clasificada nacional, deberán estar sometidos exclusivamente a la jurisdicción española.

157. En el caso de sistemas que manejen **exclusivamente** información clasificada de otros ámbitos deberán cumplirse las restricciones de sometimiento jurisdiccional impuestas por la normativa que sea de aplicación.

7.1.3.2.3 D3: COPIAS DE SEGURIDAD (BCK) - L2

158. En el caso de información clasificada, será aplicable todo lo descrito en el apartado 7.1.2.2.3 D3: COPIAS DE SEGURIDAD (BCK) –L1. No obstante, se exigirá que la gestión de las copias de seguridad **sea realizada por el CSC** y no se delegue en el CSP.

7.1.3.2.4 D4: GESTION DE LA CONFIGURACIÓN (GCF) – L2

159. Los Sistemas y elementos del Sistema deberán provisionarse con una configuración conocida y aprobada. Dicha configuración podrá ser modificada por el responsable del Sistema en todo momento.

160. **En ningún caso se podrán utilizar sistemas operativos que no dispongan de soporte de seguridad del fabricante o que no estén aceptados por la Autoridad de Acreditación.**

7.1.3.2.5 D5: PROTECCIÓN DE LAS COMUNICACIONES (PCM) – L2

161. Deberán aplicarse mecanismos criptográficos para la protección de la confidencialidad, integridad de la información en tránsito y autenticación extremo a extremo, mediante la utilización de redes privadas virtuales (VPN) que hayan **superado con éxito un proceso de aprobación**. La utilización de cifrado *on line* será obligatoria siempre que se envíe información fuera del Sistema clasificado DIFUSIÓN LIMITADA.

162. Todos los **productos o servicios de cifrado *on line* utilizados deberán estar incluidos en el CPSTIC,** en el apartado de productos o servicios aprobados para el grado de clasificación DIFUSIÓN LIMITADA o superior.

7.1.3.2.6 D5: PROTECCIÓN DE SOPORTES (PSI) – L2

163. Todos los productos o servicios de **cifrado en reposo** deberán estar incluidos en el CPSTIC en el apartado de **Productos o Servicios Aprobados** para el manejo de información DIFUSIÓN LIMITADA o superior.

7.1.3.2.7 D5: GESTIÓN DE CLAVES (GCK) – L2

164. Para la gestión de claves criptográficas se utilizarán dispositivos HSM (*Hardware Security Modules*), que deberán **haber superado con éxito un proceso de aprobación**. Se utilizarán claves generadas por el usuario, que se rotarán periódicamente, de acuerdo al Plan de Gestión de Claves asociado al producto.

165. Todas las claves criptográficas que se encuentren en uso deberán almacenarse de manera segura, utilizando mecanismos aprobados que presenten, al menos, la misma fortaleza que la de las claves.

7.1.3.2.8 D7: FIREWALL DE APLICACIÓN WEB (WAF) – L2

166. El CSC será el responsable del despliegue de un firewall de aplicación para proteger sus recursos, que debe haber sido aprobado para manejar información DIFUSIÓN LIMITADA.

7.1.3.2.9 D7: BORRADO SEGURO DE DATOS (BSD) – L2

167. Se implementarán mecanismos de borrado seguro que permitan al usuario eliminar la información de manera que no sea recuperable una vez que finalice su uso.

168. Las herramientas utilizadas para el borrado debeberán estar incluidas en el listado de Productos Aprobados del CPSTIC.

169. Para la sanitización de soportes que manejan información clasificada deberá cumplirse con lo establecido en la guía ***CCN-STIC-305 Destrucción y Sanitización de soportes informáticos*** [9] para el grado de clasificación del Sistema que se desee sanitizar.

7.1.3.2.10 D9: GESTION DE USUARIOS (GUS) – L2

170. Para la gestión de usuarios será aplicable todo lo descrito en el apartado 7.1.2.2.10 D9: GESTION DE USUARIOS (GUS) – L1. Además, se exigirá que:

    c) Los sistemas o equipos desde el que un usuario administrador administra el servicio deberá estar acreditado al mismo nivel de clasificación.

    d) Se exigirá que todas las personas del CSC con privilegios de acceso al sistema como administrador dispongan de HPS expedida por la ANS con nivel igual o superior al de la información que vaya a manejar el sistema.

7.1.3.2.11 D10: CONTROL DE SESIÓN (CSS) – L2

171. Además de lo indicado en el apartado 7.1.2.2.14 D10: CONTROL DE SESIÓN (CSS) – L1, antes del establecimiento de una sesión en el Sistema deberá aparecer un mensaje advirtiendo que solo los usuarios autorizados pueden acceder al Sistema y que la actividad será supervisada para asegurar el cumplimiento de la política de

seguridad. En dicho mensaje no se facilitará información del Sistema que pueda identificarlo o caracterizarlo ante un atacante.

7.1.3.2.12 D12: AISLAMIENTO DE DATOS Y RECURSOS (ADR) – L1

172. Consistirá en un conjunto de medidas/opciones de configuración implementadas entre los diferentes sistemas VMs/*host*, destinadas a impedir que se produzca una transferencia de información o tráfico no controlada. La compartición de recursos y datos entre el dominio de seguridad DIFUSIÓN LIMITADA y otros (ya sean también DIFUSIÓN LIMITADA o sin clasificar) deberá ser autorizada expresamente.

173. En este sentido, se exigirá, cuando no esté autorizada:

    a) Compartimentación de las máquinas virtuales, de tal forma que no esté permitida la compartición lógica de recursos incluida la posibilidad de copiar, cortar, pegar y crear carpetas compartidas entre máquinas.

    b) Asignación estática de los recursos de memoria y almacenamiento. En caso de que sea necesario reasignar recursos de una máquina a otra de menor grado de clasificación, deberán utilizarse los mecanismos de sanitización descritos en la guía CCN-STIC-305 *Destrucción y Sanitización de soportes informáticos* [9] para el grado de clasificación del Sistema que se desee sanitizar.

7.1.3.2.13 D12: PROTECCIÓN DEL PERIMETRO (PDP) – L2

174. Siempre que el Sistema gestionado por el consumidor se interconecte con otros sistemas, deberán utilizarse los dispositivos de protección de perímetro requeridos en la **CCN-STIC-302** [6] **para la interconexión para sistemas DIFUSIÓN LIMITADA.**

175. Es importante destacar que se considerará interconexión el intercambio de información entre máquinas virtuales de distintos grados de clasificación o del mismo grado pero de distinta autoridad operativa de seguridad TIC, por lo que deberán compartimentarse, incluida la posibilidad de copiar, cortar y pegar entre ellas, de tal forma que toda la información se intercambie a través de los dispositivos de protección de perímetro utilizados.

176. Estos dispositivos / servicios de protección de perímetro deberán figurar entre los productos / servicios aprobados del CPSTIC.

7.1.3.2.14 D12: SEGREGACIÓN DE REDES (SGR) – L2

177. Se utilizarán nubes privadas virtuales, configuradas por el CSC para incrementar el nivel de aislamiento ofrecido por el CSP entre los sistemas de los diferentes *tenats*. Estas VPC consisten en un conjunto de medidas basadas en la utilización de distintas subredes, así como en el establecimiento de canales seguros para cada *tenant*. De esta forma, se establecen nubes virtuales privadas mediante *software* que simulan una infraestructura dedicada para cada usuario.

7.1.3.2.15 D17: GESTIÓN DEL *ENDPOINT* (GEP) – L2

178. Se implementarán las medidas de bastionado descritas en la guía *CCN-STIC-498 Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro)* [3], para sistemas DIFUSIÓN LIMITADA.

7.1.4 ARQUITECTURA 1.3: IaaS PARA MANEJAR INFORMACIÓN CONFIDENCIAL O SUPERIOR

179. En esta sección, se definen las medidas de una arquitectura IaaS para manejar **información clasificada CONFIDENCIAL O SUPERIOR en la nube.**

180. En el siguiente esquema se presenta un resumen de las medidas que es necesario implementar para esta arquitectura.

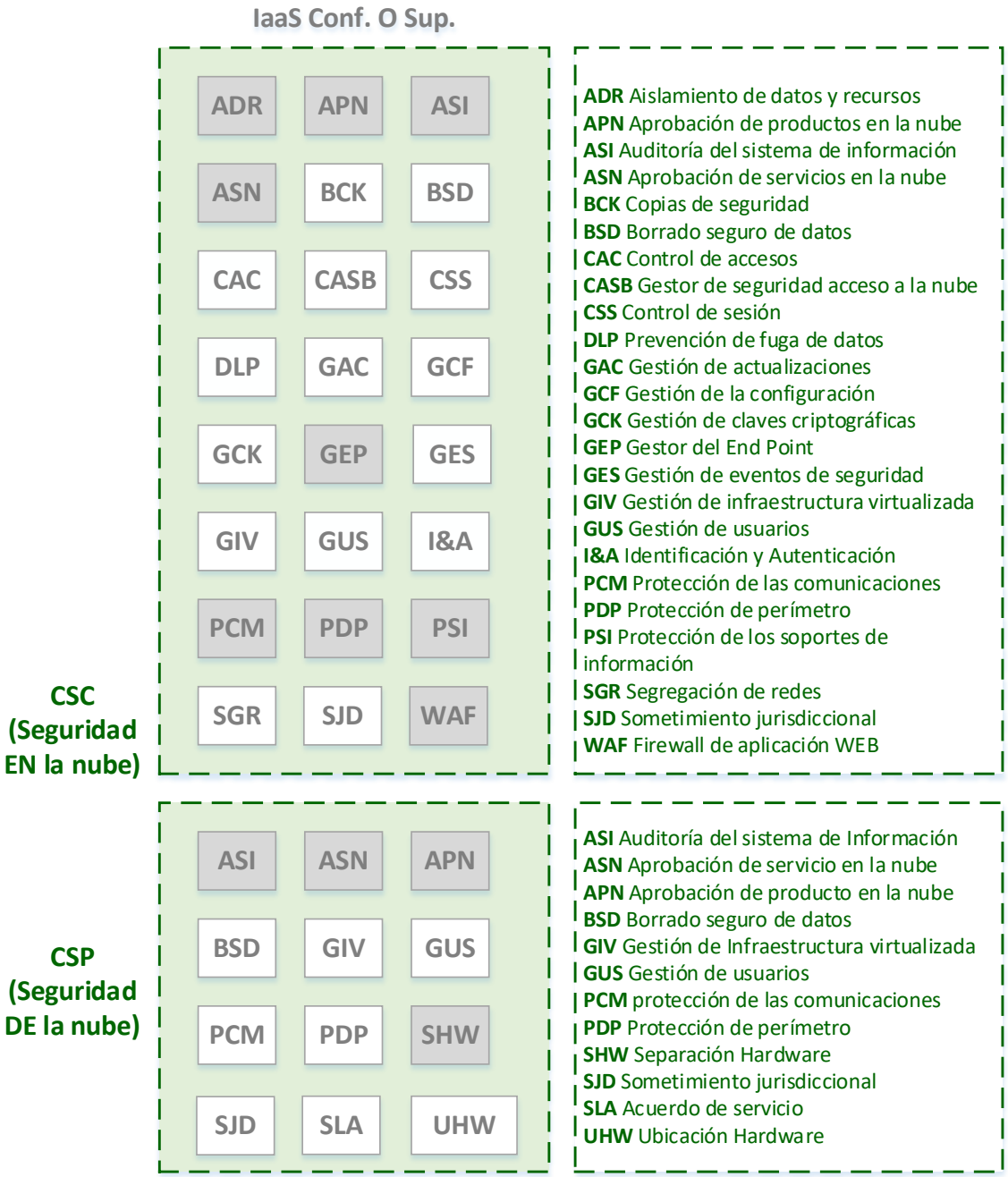


Figura 4. Medidas de Seguridad IaaS en nube Confidencial o superior

181. **Se han resaltado en gris aquellas medidas nuevas o que han sufrido modificaciones con respecto a la arquitectura de nube DIFUSIÓN LIMITADA descrita en la Sección 7.1.3 (medidas nivel L3). Estas medidas son descritas a continuación. El resto de medidas permanecen invariables y será aplicable lo descrito anteriormente.**

182. Para implementar una arquitectura segura para el escenario en el que el/los sistemas manejen información clasificada CONFIDENCIAL O SUPERIOR en la nube,

se aplicarán **todas las medidas del modelo de arquitectura descrita en la sección anterior y los elementos adicionales definidos a continuación**.

183. En el ANEXO C se incluye un diagrama detallado de alto nivel que cubre las medidas de seguridad que se definen en la siguiente sección.

7.1.4.1 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSP

7.1.4.1.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L3

184. Todos los sistemas que manejen información CONFIDENCIAL o SUPERIOR **deberán estar acreditados por la Autoridad de Acreditación Nacional de acuerdo con la guía *CCN-STIC-001 Política de Seguridad de las TIC*** [8]**.**

185. Es importante destacar que, para lograr dicha acreditación, tanto los locales en los que se instala el sistema como los equipos que manejan información clasificada deberán haber obtenido sus correspondientes certificaciones TEMPEST.

7.1.4.1.2 D2: APROBACIÓN DE SERVICIO EN LA NUBE Y APROBACIÓN DE PRODUCTO (ASN Y APN) – L3

186. Los servicios de seguridad ofrecidos por el CSP deberán estar **aprobados e incluidos en el listado de Servicios Aprobados del CPSTIC para, al menos, el grado de clasificación** de la información que vaya a manejar el Sistema.

7.1.4.1.3 D12: SEPARACIÓN *HARDWARE* (SHW) – L2

187. Cuando se vaya a manejar información CONFIDENCIAL O RESERVADO, se podrá compartir *hardware* en aquellos casos en los que exista una **autorización expresa**.

188. En general, se podrá compartir *hardware* entre sistemas que manejen información clasificada hasta RESERVADO, pertenecientes a un mismo organismo (**nube privada**) o a diferentes organismos que pertenezcan a una comunidad autorizada, cuyos miembros se determinarán mediante acuerdos cuando se establezca la arquitectura de nube (**nube comunitaria**).

189. **En ningún caso será posible compartir *hardware* con sistemas que manejen información sin clasificar.**

190. **En ningún caso, un sistema SECRETO podrá compartir *hardware con ningún otro sistema de otro nivel de clasificación*.**

7.1.4.2 MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR EL CSC

7.1.4.2.1 D1: AUDITORÍA DEL SISTEMA DE INFORMACIÓN (ASI) – L3

191. Todos los sistemas que manejen información CONFIDENCIAL o SUPERIOR **deberán estar acreditados por la Autoridad de Acreditación Nacional de acuerdo con la guía *CCN-STIC-001 Política de Seguridad de las TIC*** [8]**.**

7.1.4.2.2 D2: APROBACIÓN DE SERVICIO EN LA NUBE Y APROBACIÓN DE PRODUCTO (ASN Y APN) – L3

192. Siempre que sea posible, en la arquitectura de seguridad del Sistema se utilizarán productos o servicios que hayan sido incluidos como **productos o servicios aprobados en el CPSTIC para, al menos, el grado de clasificación** de la información que vaya a manejar el Sistema.

7.1.4.2.3 D5: PROTECCIÓN DE LAS COMUNICACIONES (PCM) – L3

193. Deberán aplicarse mecanismos criptográficos para la protección de la confidencialidad, integridad de la información en tránsito y autenticación extremo a extremo, mediante la utilización de redes privadas virtuales (VPN) que hayan **superado con éxito un proceso de aprobación**. La utilización de cifrado *on line* será obligatoria siempre que se envíe información fuera del Sistema clasificado.
194. Todos los productos o servicios de cifrado *on line* utilizados deberán estar incluidos en el CPSTIC, en el apartado de productos o servicios aprobados para el grado de clasificación igual o superior al de la información que vaya a manejar el Sistema.

7.1.4.2.4 D5: PROTECCIÓN DE SOPORTES (PSI) – L3

195. Todos los productos o servicios de cifrado en reposo deberán estar incluidos en el CPSTIC en el apartado de **Productos o Servicios Aprobados** para el manejo de información del grado de clasificación correspondiente.

7.1.4.2.5 D7: *FIREWALL* DE APLICACIÓN WEB (WAF) – L3

196. El CSC será el responsable del despliegue de un *firewall* de aplicación para proteger sus recursos, que debe haber sido aprobado el grado de clasificación que corresponda.

7.1.4.2.6 D12: AISLAMIENTO DE DATOS Y RECURSOS (ADR) – L2

197. Consistirá en un conjunto de medidas/opciones de configuración implementadas entre los diferentes sistemas VMs/*host*, destinadas a impedir que se produzca una transferencia no controlada. La compartición de recursos y datos entre el dominio de seguridad CONFIDENCIAL o RESERVADO y otros (del grado de clasificación que sean salvo SECRETO) deberá ser autorizada expresamente.

198. En este sentido, se exigirá, cuando no esté autorizada:

a) Compartimentación de las máquinas virtuales, de tal forma que no esté permitida la compartición lógica de recursos incluida la posibilidad de copiar, cortar, pegar y crear carpetas compartidas entre máquinas. Por norma general, no podrán convivir en un mismo *host* máquinas virtuales que manejen información clasificada con otras sin clasificar.

b) Asignación estática de los recursos de memoria y almacenamiento. En caso de que sea necesario reasignar recursos de una máquina a otra de menor grado de clasificación, deberán utilizarse los mecanismos de sanitización descritos en la guía *CCN-STIC-305 Destrucción y Sanitización de soportes informáticos* [9] para el grado de clasificación del Sistema que se desee sanitizar.

199. En ningún caso, un sistema SECRETO podrá virtualizarse con otro sistemas de otro nivel de clasificación.

7.1.4.2.7 D12: PROTECCIÓN DEL PERIMETRO (PDP) – L3

200. Siempre que el Sistema gestionado por el CSC se interconecte con otros sistemas, deberán utilizarse los dispositivos de protección de perímetro requeridos en la CCN-STIC-302 [6] para la interconexión de sistemas del grado de clasificación correspondiente.

201. Por ejemplo, si el CSP dispusiera de varios CPD para dar los servicios Cloud, estos deberán interconectarse siguiendo los requisitos indicados en la CCN-STIC-302 [6]. En ningún caso se permitirá que la infraestructura base del Cloud disponga de acceso directo a internet u otras redes ajenas al CSP sin utilizar los mecanismos de interconexión adecuados en función del nivel de clasificación de la Información.

202. Es importante destacar que se considerará interconexión el intercambio de información entre máquinas virtuales de distintos grados de clasificación, por lo que deberán compartimentarse, incluida la posibilidad de copiar, cortar y pegar entre ellas, de tal forma que toda la información se intercambie a través de los dispositivos de protección de perímetro utilizado.

203. Estos dispositivos/servicios de protección de perímetro deberán figurar entre los productos/servicios aprobados del CPSTIC para el grado de clasificación correspondiente.

7.1.4.2.8 D17: GESTIÓN DEL *ENDPOINT* (GEP) - L3

204. Se implementarán las medidas de bastionado descritas en la guía CCN-STIC-498 *Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro)* [3] para sistemas del nivel de clasificación considerado.

205. Además, dado que se accede a información clasificada desde el Endpoint, este deberá encontrarse dentro de una Zona de Acceso Restringido.

7.1.5 RESUMEN: TIPOS DE NUBE POR ARQUITECTURA

206. Teniendo en cuenta las distintas categorías de servicio, así como las medidas contempladas en cada una de las arquitecturas planteadas, la siguiente tabla presenta un resumen de los modelos de despliegue que serían aplicables para cada una de ellas:

	IAAS	PAAS	SAAS
SIN CLASIFICAR	Nube pública, privada o comunitaria	Por definir	Por definir
DIFUSIÓN LIMITADA	Nube privada o comunitaria	Por definir	Por definir
CONFIDENCIAL O SUPERIOR	Nube privada o comunitaria	Por definir	Por definir

8. DEFINICIONES

Información Roja	Información clasificada y que, por lo tanto, requiere protección de acuerdo a la Normativa Protección de Información Clasificada generada por la Oficina Nacional de Seguridad.
Información Negra	Información no clasificada o información clasificada que ha sido cifrada con mecanismos de cifra aprobados por la autoridad competente y que, por lo tanto, puede protegerse con los mismos medios que la información no clasificada.
Información sensible	Información que demanda un alto nivel de seguridad en alguna de sus dimensiones.
Información Clasificada	Asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado.
Ámbito de seguridad	Ámbito de origen al que pertenece la información, es decir, la organización o nación propietaria de la información clasificada a la que puede tener acceso, si es necesario. Por ejemplo: OTAN, UE o NACIONAL.
Nivel de seguridad	Máxima clasificación de la información clasificada dentro de un mismo ámbito de seguridad.
Dominio de seguridad	Ámbito de seguridad o nivel de seguridad dentro de un mismo ámbito.
Nube privada virtual	Una nube privada virtual (VPC) es una versión virtual de una red física, implementada dentro de la red del CSP.

9. REFERENCIAS

[1] AC/322(CP/4)WP(2021)0003-REV2 DRAFT Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-Based Communication and Information Systems (CIS).

[2] CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).

[3] CCN-STIC-498 Arquitectura mulidominio de Puesto de Trabajo (Endpoint Seguro).

[4] CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[6] CCN-STIC 302 Interconexión de Sistemas TIC que manejan Información nacional clasificada en la administración, Julio 2012.

[7] CCN-STIC-301 Medidas de Seguridad de las TIC a implementar en Sistemas Clasificados, Mayo 2020.

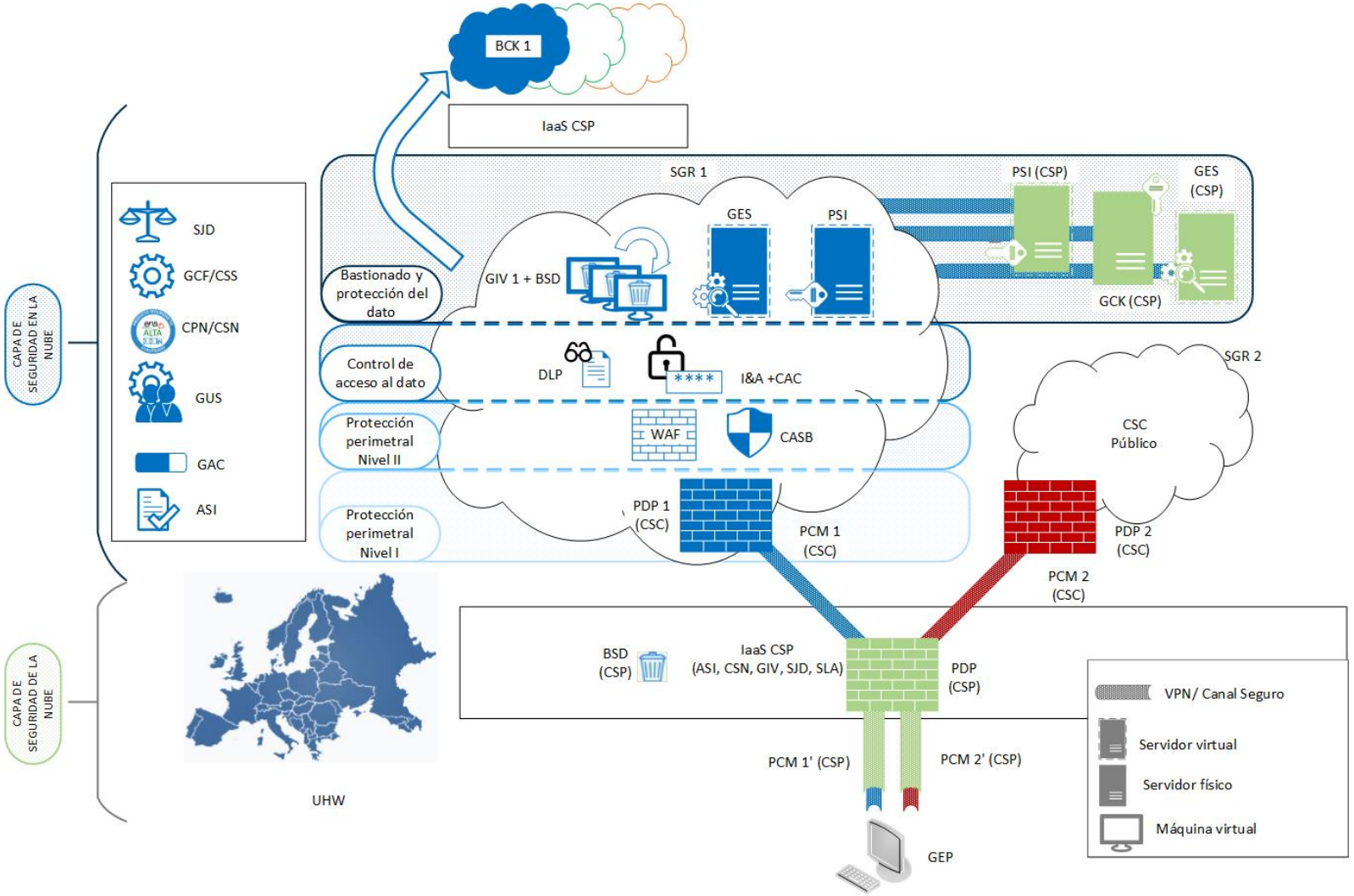
[8] CCN-STIC-001 Política de Seguridad de las TIC, Junio 2016.

[9] CCN-STIC-305 Destrucción y Sanitización de soportes informáticos, Mayo 2017.

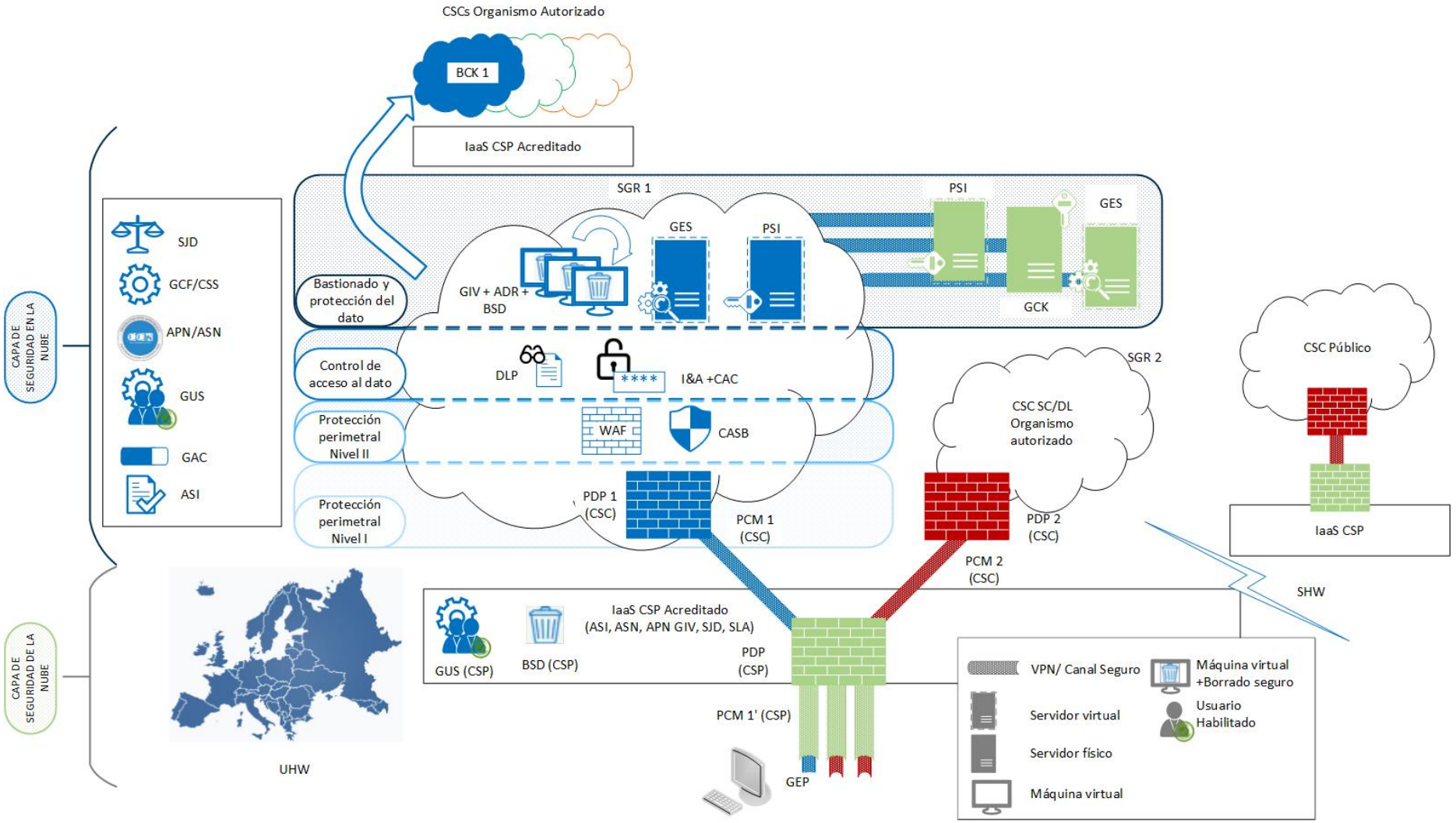
10.ABREVIATURAS

CASB	*Cloud Access Security Broker*
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSC	*Cloud Service Customer*
CSP	*Cloud Service Provider*
DLP	*Data Loss Prevention*
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
ENS	Esquema Nacional de Seguridad
HPS	Habilitación Personal de Seguridad
HSM	*Hardware Security Modules*
HTTPS	*Hypertext Transfer Protocol Secure*
IaaS	*Infrastructure as a Service*
KMS	*Key Management System*
MV	Máquina Virtual
ONS	Oficina Nacional de Seguridad
PaaS	*Platform as a Service*
PES	Procedimiento de Empleo Seguro
RPO	*Recovery Point Objetive* (Objetivo punto de recuperación)
RTO	*Recovery Time Objetive* (Objetivo tiempo de recuperación)
SaaS	*Software as a Service*
SLA	Acuerdo de servicio
SO	Sistema Operativo
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*
VM	*Virtual Machine*
VPN	*Virtual Private Network*

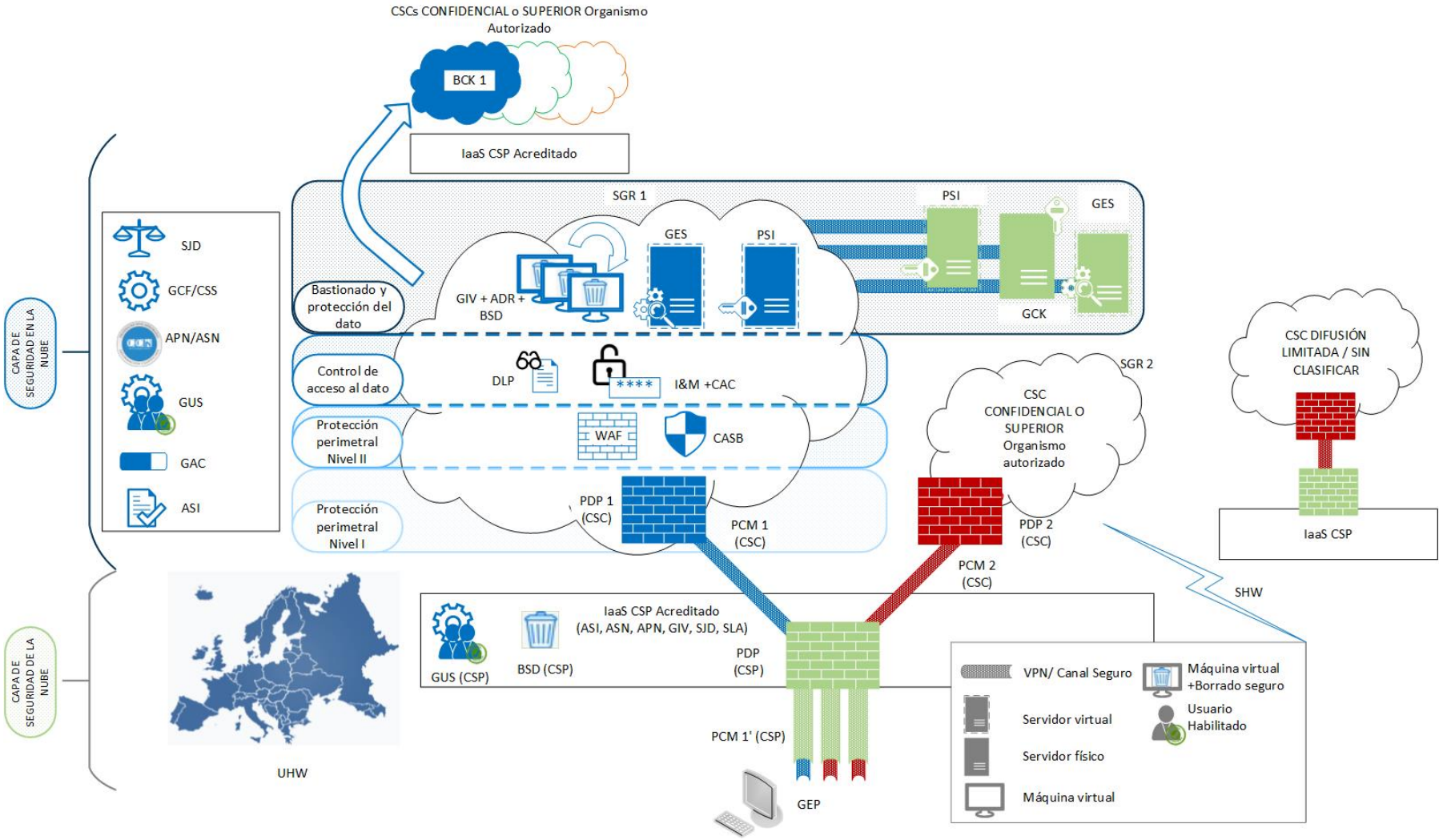
ANEXO A. DIAGRAMA IaaS PARA MANEJAR INFORMACIÓN SIN CLASIFICAR



ANEXO B. DIAGRAMA IaaS PARA MANEJAR INFORMACIÓN DIFUSIÓN LIMITADA



ANEXO C. DIAGRAMA IaaS PARA MANEJAR INFORMACIÓN CONFIDENCIAL O SUPERIOR



PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL