Guía de Seguridad de las TIC
CCN-STIC 858

Implantación de sistemas en modo local (*on-premise*)



Noviembre 2026

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2026

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.11.12 13:19:14 +01'00'

Fecha de Edición: noviembre de 2026

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 4
2. OBJETO 4
3. ALCANCE 5
4. IDENTIFICACIÓN Y ACTUALIZACION DE LAS GUIAS 5
5. GUÍA DE INSTALACIÓN Y CONFIGURACIÓN SEGURA DEL SISTEMA 5
5.1 PRESENTACIÓN Y ARQUITECTURA DE LA SOLUCIÓN 6
5.2 ACCIONES NECESARIAS DE LOS ADMINISTRADORES EN LA INSTALACIÓN 6
5.3 MANUAL DEL ADMINISTRADOR 6
5.4 DIMENSIONAMIENTO DE LA SOLUCIÓN 7
5.5 CÓMO ESTABLECER UNA CONFIGURACIÓN INICIAL SEGURA 8
5.6 CONSIDERACIONES PARA ACTUALIZAR EL SISTEMA 8
5.7 CÓMO REALIZAR PRUEBAS DE INTEGRIDAD DEL SISTEMA 8
5.8 REQUISITOS DE SEGURIDAD 8
5.9 REQUISITOS DE SEGURIDAD Y CONTROLES DEL ENS IMPLEMENTADOS 9
5.10 COMUNICACIÓN DE INCIDENCIAS Y SOLICITUD DE SOPORTE 9
5.11 CUALQUIER OTRO ASPECTO PARA MEJORAR DE LA SEGURIDAD 9
6. GUÍA DE USO SEGURO DEL SISTEMA 10
6.1 APROXIMACIÓN A LA NORMATIVA DE USO DEL SISTEMA. 10
6.2 CONFIGURACIONES Y PROCEDIMIENTOS DE SEGURIDAD QUE DEBAN SER REALIZADAS POR LOS USUARIOS 10
6.3 COMUNICACIÓN DE INCIDENCIAS Y SOLICITUD DE SOPORTE 10
6.4 MANUAL DE USUARIO 10
7. GUÍA DE RELACIÓN ENTRE PROVEEDOR Y CLIENTE 10
7.1 ASIGNACIÓN DE LA RESPONSABILIDAD DE CADA PARTE RESPECTO AL ANEXO II DEL ENS 11
7.2 ANÁLISIS DE RIESGOS DE LA SOLUCIÓN IMPLANTADA 11
8. ANEXO I. EJEMPLO DE ASIGNACIÓN DE RESPONSABILIDADES ENTRE PROVEEDOR Y CLIENTE 13
9. ANEXO II. EJEMPLO PARA CONFECCIONAR EL ANÁLISIS DE RIESGOS DE LA SOLUCIÓN IMPLANTADA 36

1. INTRODUCCIÓN

Es una tendencia creciente considerar a la cadena de suministro fundamental para la seguridad de las organizaciones, como refrenda el que lo contemplen cada vez mayor número de normas jurídicas y de marcos o 'frameworks' de ciberseguridad

A modo de ejemplo podemos citar la Directiva de la UE 2022/2555 (NIS2) y el propio RD 311/2022 (ENS); además de la ISO 27001:2022, el NIST CSF 2.0, el CSA Cloud Control Matrix v4.1, etc.

La dificultad radica en que, en ocasiones, resulta difícil abarcar todos los posibles casos de uso que pueden llegar a darse. Es por esta razón que, en junio de 2020, el Centro Criptológico Nacional, publicó la primera edición de esta guía que ahora se actualiza, entre otras razones, para armonizarla con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Su finalidad última es aportar recursos que mejoren la seguridad de aquellas organizaciones que contratan servicios / aplicaciones externalizadas que, en vez de suministrarse desde la Nube, es decir, en modalidad de software como servicio (SaaS), se instalarán localmente sobre la propia infraestructura de la organización cliente que las contrata, en sus instalaciones físicas, lo que se conoce como implantación o despliegue *en modo local* (en inglés ON-PREMISE).

Mientras que en las soluciones que se prestan desde la Nube en modalidad SaaS la materialización de las medidas de seguridad corresponde en gran medida al proveedor prestador del servicio (CSP), o al menos en una elevada proporción de lo que se conoce como '*responsabilidad compartida*', en las soluciones implantadas ON-PREMISE las medidas de seguridad asimismo se reparten entre ambos: el proveedor que suministra el servicio y la organización cliente que lo contrata, aunque con mayor proporción para ésta última.

En el anexo I, al final de esta guía, se detalla una propuesta de reparto de la referida responsabilidad de implantar las correspondientes medidas de seguridad, que debe tomarse como una orientación que puede variar en función del caso particular, por lo que cada proveedor la ajustará antes de entregarla y, en su caso, consensuarla con su cliente ante posibles discrepancias.

NOTA: Debe considerarse que el hecho de que un proveedor del sector privado esté en posesión de la correspondiente certificación de conformidad con el ENS que abarque los servicios soportados por su sistema de información, junto con el hecho de que una organización cliente realice una adecuada instalación de la solución externalizada conforme a las pautas de seguridad dadas por el proveedor, así como siguiendo esta guía, no le eximirán en ningún caso a esta última de sus obligaciones con respecto a la certificación de la conformidad de su propio sistema de información respecto al ENS.

2. OBJETO

El objeto de esta guía es desarrollar lo que se ha planteado en la Guía de Seguridad '**CCN-CERT IC-01/19 ENS: Criterios adicionales de auditoría y certificación**' que señala: "*En relación con la evaluación de sistemas SaaS implantados en modo local, se recuerda la obligatoriedad de que la EC/OAT contemple, cuando proceda, lo dispuesto en la Guía*

CCN-STIC 858, incluyendo la evaluación del contenido de la preceptiva 'Guía de relación entre cliente y proveedor' que allí se menciona". Quiere esto decir que no se concederá la certificación del ENS a un proveedor de soluciones implantadas en modo local si no dispone y entrega a sus clientes un ejemplar de las tres guías que en este documento se describen.

Cada proveedor de soluciones implantadas en sus clientes en modo local (ON-PREMISE) deberá adaptar el contenido de las tres guías referenciados en este documento a su realidad concreta, considerando que ésta es su finalidad: Permitir conocer la seguridad inherente en la solución aportada, posibilitando adaptarla y complementarla con la necesaria en la organización cliente.

No obstante, hay que señalar que para que el sistema de información del proveedor de servicios pueda alcanzar la Certificación de Conformidad con el ENS, será necesario que se verifique la idoneidad de las adaptaciones concretas que se hayan realizado y que, en consecuencia, se tomen como otro requisito añadido a tener en cuenta para poder otorgarle la referida Certificación. Concretamente, se verificarán la Guía de instalación, la Guía de uso seguro y la Guía de relación entre proveedor y cliente.

3. ALCANCE

Por practicidad, se han analizado en un único documento las tres guías que se considera necesario que el proveedor de la solución implantada en modalidad ON-PREMISE entregue a su cliente: La **Guía de instalación** (dirigido a administradores), la **Guía de uso seguro** (dirigido a usuarios) y la **Guía de relación entre proveedor y cliente** (dirigida al Responsable de Seguridad y al Responsable del Sistema).

En la práctica de su actividad profesional, e**l proveedor de la solución entregará a su cliente las tres (3) guías claramente diferenciadas**, dado que se dirigen a perfiles o colectivos distintos: Administradores; usuarios; y Responsable de Seguridad y del Sistema.

4. IDENTIFICACIÓN Y ACTUALIZACION DE LAS GUIAS

Las tres guías que deben proporcionarse al cliente están sujetas a la evolución de las soluciones suministradas, a la tecnología subyacente o utilizada en cada caso y a lo dispuesto en el propio ENS y sus normas de desarrollo. En consecuencia, el proveedor debe mantener las Guías permanentemente actualizadas y proporcionar, o poner a disposición de sus clientes, las nuevas versiones que estén disponibles y que se correspondan con los sistemas provistos a sus clientes.

Para ello se identificará claramente la versión y fecha de cada una de ellas, así como la solución a la que va destinada. Siempre que sea posible, se incluirá un apartado inicial donde se resuman los cambios más significativos respecto a la versión anterior.

5. GUÍA DE INSTALACIÓN Y CONFIGURACIÓN SEGURA DEL SISTEMA

Esta guía está dirigida a los administradores del Sistema de Información del cliente que contrata, para posibilitar la integración en la infraestructura tecnológica de dicho

cliente de un sistema, subsistema o solución, provista por un proveedor externo, a la que llamaremos "***solución implantada***", bien haya sido desarrollada por el propio proveedor o por un tercero. En cualquier caso, la implementación habitualmente no la realizará el propio cliente, aunque participe, sino el proveedor.

Esencialmente, el objeto de la citada Guía es instruir sobre el proceso de instalación y parametrización de la solución implantada, de manera que se mantenga la seguridad en su conjunto y en todas las dimensiones de la misma. Por este motivo, los administradores de la organización cliente podrán encontrar en la Guía la información adecuada relativa a la interconexión de la solución con el resto de la arquitectura e infraestructura del cliente, incluyendo aplicaciones, activos relacionados con la tecnología y otros componentes para manejar la información.

Además, la citada Guía también podrá aportar recomendaciones de configuración de otros activos no provisionados con la solución, pero que forman parte de la red de la organización cliente donde se implanta y son necesarios para asegurar el funcionamiento global. Todo esto sin olvidar la posible interoperabilidad que se requiera con otros sistemas.

5.1 Presentación y arquitectura de la solución

- Se describirá la solución global, se mostrará gráficamente su arquitectura y se describirán lo más detalladamente posible todos los módulos y elementos en que se estructura, junto a las relaciones entre ellos.
- Se describirá, asimismo, la infraestructura necesaria en el cliente para soportar la solución.
- Se describirá la integración de ambas infraestructuras (de la solución y del cliente), proporcionándose advertencias de seguridad y de los posibles riesgos derivados de su interacción.

5.2 Acciones necesarias de los administradores en la instalación

Se detallarán todas aquellas acciones necesarias por parte de los administradores del sistema de información del cliente, que se requieren para implantar la solución, así como para su posterior mantenimiento.

Además de incluir los extremos necesarios relativos a la configuración y parametrización inicial de la solución implantada, el proveedor deberá indicar aquellas precisiones o cautelas de las que tenga conocimiento y que, a su juicio, deban ser adoptadas por el cliente en relación con otros productos que tenga instalados en su infraestructura tecnológica y que deban interaccionar con la solución implantada.

5.3 Manual del administrador

Se describirá todo lo necesario que debe conocer un administrador de la organización cliente, para poder desarrollar sus responsabilidades respecto de la solución implantada, durante todo su ciclo de vida.

Incidirá en aspectos tales como:

- Estructuración y gestión de usuarios y grupos, junto a la asignación de derechos de acceso.
- Configuración del nivel de detalle, contenido y funcionalidades que alimenten las trazas de auditoría y posibilidades de consulta y exportación.
- Configuración de mecanismos de autenticación y su fortaleza, prestando atención, si procede, a multifactor de autenticación (MFA), LDAP, etc.
- Acceso remoto seguro.
- Consejos de bastionado e información de seguridad por defecto (SbD) y Privacidad por Defecto (PbD).
- Instalación de aplicaciones de la solución en servidores y, en su caso, en los clientes de la red.
- Configuración de conexiones internas y externas, incluyendo APIs y posible envío de correos electrónicos y mensajes SMS.
- Desinstalación de productos.
- Metadatos en los documentos generados y/o almacenados.
- Purgado de las tablas de Base de Datos, automático o manual, con posibles parametrizaciones y gestión de plazos de conservación.
- Implicaciones de protección de datos; y cualesquiera otros aspectos que se considere relevante incluir.

La ausencia en este Manual del Administrador de cualquier contenido del que pudiera derivarse una inadecuada configuración del sistema y que pudiera comportar daños o perjuicios para la entidad cliente o para los servicios prestados, será responsabilidad del proveedor de la solución.

5.4 Dimensionamiento de la solución

Se dará toda la información y tablas necesarias para que los administradores del cliente puedan dimensionar los recursos necesarios para la instalación y uso del sistema, evitando la falta de disponibilidad de los mismos, ya sea de forma inicial o durante todo su ciclo de vida.

Deben considerarse los recursos necesarios en relación con:

- El procesador.
- La Memoria.
- Nº de servidores físicos o virtuales.
- Almacenamiento.
- Ancho de banda de comunicaciones.
- Recursos de personal o accesorios hardware necesarios si procede, etc.

En función de parámetros claros:

- Nº de usuarios.
- Nº de registros a ser tratados diariamente.
- Nº de trámites, etc.

5.5 Cómo establecer una configuración inicial segura

Para alcanzar un funcionamiento seguro de la solución contratada y del resto del sistema en el que se integra, se considerarán tanto aquellos aspectos de configuración de la propia solución, como de los elementos comunes de la infraestructura que la soporta.

A modo de ejemplo, sin que se trate de una relación cerrada, se indicará:

- Subredes necesarias.
- Direccionamiento IP.
- Puertos empleados.
- Mecanismos de autenticación.
- Parámetros de la base de datos.
- Etc.

En este sentido, se utilizarán diagramas capaces de presentar estos conceptos de forma clara.

5.6 Consideraciones para actualizar el sistema

En este apartado se informará del mecanismo que dispone el proveedor para notificar la aparición de parches de seguridad, incluyendo las vulnerabilidades corregidas y su criticidad, parches acumulativos periódicos previstos y su frecuencia, precauciones a adoptar para su instalación, verificaciones, copias de seguridad previas, etc.

También se detallarán las instrucciones específicas de actualización de versiones y el formato de las hojas de anuncio de las mismas caso de estar establecido.

5.7 Cómo realizar pruebas de integridad del sistema

Se indicarán aquí aquellas posibles pruebas de integridad durante y/o tras la instalación inicial, para garantizar que todos los elementos, ya sean los incluidos en la solución o pertenecientes a la instalación del cliente, se integren de forma correcta sin interferencias funcionales ni menoscabo de la seguridad.

5.8 Requisitos de seguridad

Se detallarán en este aquellos aspectos de la infraestructura del cliente que resulten necesarios para dotar a la solución implantada del suficiente nivel de seguridad.

Es imperativo profundizar en el nivel de detalle de todo aquello que no se corresponda con las exigencias o requisitos operativos privativos del negocio del cliente. Por ejemplo, no bastará con señalar que se requiere un firewall, sino que, cuando la acción deba ser responsabilidad del proveedor, habrá de especificarse el número de subredes a configurar, los puertos que se requieren abiertos de entrada y salida y su finalidad, direccionamientos, posibles reglas a definir en los firewalls, etc.

Los requisitos se determinarán en función de la categoría de seguridad del sistema. Por ejemplo, la forma permitida de implementar las subredes dependerá de la categoría del sistema según se determina en la medida [mp.com.4] del ENS.

5.9 Requisitos de seguridad y controles del ENS implementados

Se detallarán en este apartado, de forma resumida, aquellos aspectos de cada medida de seguridad del Anexo II del ENS que resulten de aplicación atendiendo a la categoría de seguridad del sistema, en el caso de que se satisfagan de origen.

Caso de no ser así, se indicará la alternativa correcta si hay más de una opción, o bien se indicará que no se cumple, por lo que el cliente deberá apoyarse en otros recursos como son las medidas compensatorias (según se determinan en la guía "**CCN-STIC 810 Medidas compensatorias**") y/o las complementarias de vigilancia.

5.10 Comunicación de incidencias y solicitud de soporte

Si el soporte a los usuarios del sistema lo proporciona un Centro de Atención al Usuario (CAU) del cliente, será éste el encargado de realizar las notificaciones de incidencias o peticiones de soporte al proveedor. Para ello se especificarán los mecanismos de notificación: teléfono, correo electrónico, formulario Web, etc., indicando el horario de atención.

Si el proveedor asume el soporte directo a los usuarios de la organización cliente donde se ha implantado la solución, se especificarán asimismo los mecanismos de contacto y un estudio de la capacidad estimada de incidencias y peticiones de servicio a tratar.

Se indicarán los SLA establecidos, en función de la urgencia de la incidencia o petición de servicio, prestando especial atención a los incidentes de seguridad.

5.11 Cualquier otro aspecto para mejorar de la seguridad

Se detallará en este apartado cualquier otro aspecto a considerar para la mejora de la seguridad, denotando sus ventajas e indicando si se trata de una práctica habitual para este tipo de soluciones.

También se detallarán aquellos módulos o complementos de seguridad que, siendo opcionales, no se incluyen en la solución de base y deban ser contratados aparte, señalándose igualmente los beneficios de su incorporación y los riesgos de no hacerlo.

Para sistemas de categoría MEDIA o ALTA, podría indicarse aquí todo lo necesario para facilitar la elaboración de un Análisis de Impacto (BIA) al cliente, aportando el generado por el proveedor en lo que se refiere a su servicio de soporte, y quizá también el de mantenimiento correctivo, respecto a la solución implantada.

6. GUÍA DE USO SEGURO DEL SISTEMA

Esta guía está dirigida a los usuarios del sistema, subsistema o solución contratada, que se implante en la infraestructura del cliente, al objeto de disponer de todos los recursos necesarios para hacer un uso seguro de la misma.

6.1 Aproximación a la normativa de uso del sistema.

Si bien las normas de uso de medios electrónicos las establece la organización cliente que contrata la solución, en este apartado el proveedor aportará sugerencias sobre normas adecuadas a la realidad concreta de la solución, en base a su experiencia y al conocimiento que posee de la solución que se implanta.

6.2 Configuraciones y procedimientos de seguridad que deban ser realizadas por los usuarios

Se detallarán aquellas configuraciones y procedimientos de seguridad que deban ser realizados por los usuarios finales para garantizar un uso seguro del sistema.

También se indicarán posibles configuraciones adicionales, con una explicación clara del incremento o decremento de la seguridad en función de su ajuste, configuración o parametrización.

6.3 Comunicación de incidencias y solicitud de soporte

Caso de que el soporte lo proporcione directamente el proveedor de la solución, se especificarán los mecanismos de notificación por parte de los usuarios del sistema: Teléfono, correo electrónico, formulario Web, etc., indicando el horario de atención y la información identificativa que se le solicitará por parte del personal de soporte. Se prestará especial atención a los incidentes de seguridad, que se priorizarán.

Si el soporte lo proporciona un Centro de Atención al Usuario (CAU) del cliente, será éste el encargado de realizar las notificaciones de incidencias o peticiones de soporte.

6.4 Manual de Usuario

El Manual de Usuario resaltará las implicaciones de seguridad en determinadas acciones que puedan realizar los usuarios, especialmente parametrizaciones permitidas.

Se dispondrá de un apartado dedicado a consejos y buenas prácticas de seguridad en el escenario de aplicación de la solución implantada.

7. GUÍA DE RELACIÓN ENTRE PROVEEDOR Y CLIENTE

Esta Guía contendrá recomendaciones para la gestión de la relación entre proveedor de la solución y el cliente contratante, especificando la carga de responsabilidad de ambos, proveedor y cliente, para el cumplimiento de cada una de

las medidas de seguridad que determina el anexo II del ENS en función de la categoría del sistema.

Se trata de evitar que quede sin aplicarse una medida de seguridad en el sistema, subsistema o solución implantada ON-PREMISE, creyéndose erróneamente que la responsabilidad es exclusiva de la otra parte, cuando quizá es propia, o de ambas partes simultáneamente en determinada proporción de responsabilidad compartida.

7.1 Asignación de la responsabilidad de cada parte respecto al Anexo II del ENS

Se determinará la asignación de responsabilidad de cada parte, proveedor y cliente, respecto a los controles de seguridad del Anexo II del ENS que sean de aplicación, según la categoría del sistema.

Para ello se ha desarrollado una tabla en el ANEXO I de esta guía, que pueda servir de ejemplo de partida, dado que la casuística puede ser variopinta y diversa.

En la referida tabla se tiene en cuenta para cada una de las medidas de seguridad que determina el Anexo II del ENS:

- El código y descripción de la medida.
- La categoría del sistema para el que la medida es de aplicación.
- El porcentaje de responsabilidad en la aplicación de la medida entre el proveedor que provisiona la solución y el cliente dónde se implanta.
- Las acciones necesarias a ser llevadas a cabo por el proveedor.
- Las acciones a ser llevadas a cabo por el cliente.
- En determinados casos, notas de implantación.

NOTA: Cuando se particularice la tabla para ser entregada en la guía de una solución concreta, en la columna "notas de implantación" se detallarán, por ejemplo, paneles y parámetros concretos de configuración relacionados con esa medida, referencias a documentación adicional disponible al respecto, buenas prácticas de uso seguro, etc.

El reparto de responsabilidades cliente-proveedor será establecido, en primera instancia por el proveedor que aporta la guía, en base a su experiencia, aunque deberá consensuarse por ambas partes, atendiendo a las especiales circunstancias que concurran en cada caso concreto. En cualquier caso, el reparto de responsabilidades finalmente acordado deberá estar determinado en la versión final de la **Guía de Relación entre Cliente y Proveedor**.

7.2 Análisis de riesgos de la solución implantada

Se incluirá el resultado del Análisis de Riesgos del sistema, subsistema o solución implantada, considerando asimismo las posibles interacciones con otros sistemas del cliente.

El Análisis de Riesgos deberá ser realizado, conjuntamente, por el cliente y por el proveedor, asumiendo y responsabilizándose de sus resultados, en la parte que le corresponda a cada uno de ellos. Dicho Análisis de Riesgos será asimismo evaluado por la Entidad de Certificación, cuando el cliente se encuentre en un proceso de Auditoría de Certificación del ENS que involucre los sistemas de información sobre los que se prestan los servicios contratados.

A modo de ilustración se ha desarrollado una tabla en el ANEXO II de la presente guía, que puede servir de inspiración informal de algunas de las posibles amenazas que podrían afectar a una hipotética solución implantada. Asimismo, se sugieren acciones de mitigación, tanto a nivel de prevenciones durante el desarrollo por parte del proveedor, como de acciones de mitigación en manos de la organización cliente donde se implanta.

En la referida tabla se tienen en cuenta para cada riesgo identificado:

- El riesgo y su descripción.
- Las posibles consecuencias en caso de materializarse (impacto)
- Posibles acciones de mitigación por parte del proveedor (desarrollador)
- Posibles acciones de mitigación por parte de la organización cliente

Cuando se aporte el análisis de riesgos al cliente para que lo integre con su propia gestión general de riesgos, deben de recogerse únicamente las acciones de mitigación que, de forma efectiva, ha materializado el proveedor a nivel de diseño y desarrollo, y no las que hubiera podido aplicar. De esta forma, la organización cliente dispondrá de elementos de decisión para incorporar más o menos medidas propias que compensen o complementen las del proveedor.

El proveedor, respecto de su propia solución, se hará responsable de la diligencia y exactitud del Análisis de Riesgos realizado.

8. ANEXO I. Ejemplo de asignación de responsabilidades entre proveedor y cliente

Reparto de responsabilidades entre proveedor y cliente (Coordinación de aplicabilidad de medidas de seguridad del ENS						
Medida de seguridad	Categoría o nivel por dimensión	Responsabilidad		Acciones necesarias para el proveedor (PRV)	Acciones necesarias para el cliente (CLI)	Notas de implantación
		PRV	CLI			
org.1 Política de Seguridad	**TODAS**	50%	50%	El proveedor dispone de una política de seguridad de la información (PSI) accesible para el cliente, por ejemplo, en la URL: https://www.cliente.es/politica-de-seguridad, o se le ha dado a conocer por otro medio.	Existirá una PSI aprobada por el órgano superior.	La PSI del Proveedor es necesaria solo hasta que el sistema se implanta en la infraestructura del cliente. A partir de ese momento, la única PSI a considerar es la del cliente (que habrá de contemplar la presencia de sistemas on-premise y desarrollarse considerándolos).
org.2 Normativa de Seguridad	**TODAS**	50%	50%	En la Normativa Interna de uso de medios electrónicos en la organización, se incluirán capítulos o epígrafes específicos destinados a sistemas concretos. En este apartado, se incluirá la documentación necesaria para la implantación y el uso correcto de la solución para cumplir con el ENS. Los usuarios de la solución implantada disponen, por ejemplo, de una guía de uso seguro / manual de usuario, paneles de ayuda, avisos desplegables, banners o mensajes emergentes, con normas de uso denotando sus responsabilidades.	Se dispondrá de normativa documentada relacionada con el uso correcto y con el inadecuado de los activos, junto a sus responsabilidades, derechos, deberes y medidas disciplinarias. Entre esos activos podría ser necesario considerar la solución implantada on-premise.	Los usuarios deben conocer las funciones de la solución implantada y, en su caso, aceptarán las condiciones de uso de la misma.
org.3 Procedimientos de seguridad	**TODAS**	50%	50%	Se encuentran documentadas las acciones necesarias para la instalación segura de la solución, los procedimientos de administración, así como instrucciones y protocolos de uso seguro de la solución por parte de sus usuarios.	Se adecuarán / complementarán los procedimientos de seguridad de todo el sistema de información para que contemplen la solución implantada.	

org.4 Procedimiento de autorización	**TODAS**			50%	50%	Se encuentra documentado el proceso de autorizaciones, correspondiente tanto a administradores como a usuarios, ya sea en el entorno de instalación (Guía de instalación), como en el entorno de operación (Guía de uso seguro / manual de usuario).	Existirá un proceso de autorizaciones adecuado a todo el sistema de información, que incluya la solución implantada.	
op.pl.1 Análisis de riesgos	**B**	**M**	**A**	50%	50%	El proveedor dispone de una gestión propia de riesgos en la que ha considerado los procesos de diseño, desarrollo, implantación, mantenimiento y soporte de la solución. En la Guía de instalación segura que se facilita al cliente, el proveedor incluye un análisis de riesgos respecto a la solución que provee.	La organización cliente incluirá la solución implantada como activo o activos. La organización cliente dispondrá de un Análisis de Riesgos en el que incluirá los riesgos de gestionar soluciones ON-PREMISE y en su caso, cuando no se disponga de soporte del proveedor, deberán establecerse medidas en el plan de tratamiento de riesgos (PTR). Se incorporarán los riesgos identificados por el proveedor en la Guía de instalación de la solución en la gestión de riesgos global de la organización cliente.	Ambas partes (proveedor y cliente) deberán disponer de un análisis de riesgos actualizado.
op.pl.2 Arquitectura de seguridad	**B**	**M**	**A**	60%	40%	Se dispone de un mapa esquemático o diagrama con la arquitectura de la solución que se facilita en la Guía de instalación de la solución. Se contempla tanto a nivel de bloques de estructuración de los módulos software de la solución, como a nivel de arquitectura recomendada para implementar la misma (Balanceadores, servidores web, servidores de BBDD, etc.) e integrarla en la red del cliente. Se incluyen diagramas con indicación de las conexiones e interconexiones (flujos de datos) hacia otros sistemas y hacia el exterior, con indicación de cómo se han protegido, o pueden protegerse, incluyendo los protocolos de acceso empleados. Se documentarán en la Guía de instalación las recomendaciones de configuración y parametrización para mantener un nivel adecuado de seguridad.	La organización cliente dispondrá de documentación de las instalaciones, del sistema, de accesos al sistema, de la(s) red(es), de las líneas de defensa… de modo que se facilite la integración de la solución contratada.	

op.pl.3 Adquisición de nuevos componentes	**TODAS**			50%	50%	Cuando se incorporen o sustituyan elementos que afecten al desarrollo de software, como módulos o librerías, el proveedor de la solución verifica que no rompe la seguridad. Si es necesario establece acciones de formación y sensibilización.	La organización cliente dispondrá de un proceso para planificar las adquisiciones de soluciones que considere los riesgos, los elementos existentes en la arquitectura actual del sistema y las necesidades que pueden surgir de su integración.	
op.pl.4 Dimensionamiento / Gestión de la Capacidad	**B**	**M**	**A**	50%	50%	Se le entregan a la organización cliente de la solución ON-PREMISE, en la Guía de instalación, tablas para poder dimensionar los recursos que la soportarán, en función del nº de usuarios, nº de trámites y de otros parámetros que se estimen relevantes. Se dimensiona en base a recursos de procesador, memoria, capacidad en disco, recursos humanos, etc. Asimismo, la solución contempla parametrizar y elaborar estadísticas, permitiendo la monitorización del almacenamiento y gestionar la retención de la información.	La organización cliente dispondrá de un estudio con la evolución histórica de la capacidad del sistema, o Plan de Capacidad, que permita dimensionar los componentes en los que se apoyará la solución con ayuda de las tablas proporcionadas por el fabricante en la Guía de instalación.	La información de la solución se almacena en Base de Datos, siendo responsabilidad del cliente que contrata definir los umbrales de almacenamiento en su sistema y programar las alertas adecuadas cuando se alcancen dichos umbrales.
op.pl.5 Componentes certificados	**B**	**M**	**A**	100%	50%	Los productos o servicios suministrados para formar parte de la arquitectura de seguridad del sistema, deberán constar en el catálogo CPSTIC.	La organización cliente procurará que los componentes de la infraestructura TIC que interactúen con la solución implantada estén certificados si aquella lo está.	
op.acc.1 Identificación	**B**	**M**	**A**	70%	30%	La solución cubre las necesidades del cliente facilitándole la gestión de los usuarios: Identificación, estado, responsable o área a la que pertenece, roles asignados, permisos en base a dichos roles, etc.	Se procedimentará a nivel interno la gestión de los usuarios registrados en sus sistemas. El cliente deberá gestionar mediante procedimientos las altas, modificaciones y bajas de usuarios, así como las autorizaciones y notificaciones de dichos cambios.	La solución implantada dispone de mecanismos de consulta para listar los usuarios dados de alta en la aplicación. Los usuarios de la solución implantada pueden ser dados de baja o deshabilitados en cualquier momento y pueden tener definida una fecha de caducidad previamente establecida.
op.acc.2 Requisitos de acceso	**B**	**M**	**A**	50%	50%	La solución no permite que un usuario sin estar dado de alta, o sin los oportunos permisos, pueda acceder a recursos no habilitados.	La organización cliente gestionara los derechos de acceso de todo el sistema, incluidos los derechos de acceso que	

							puedan corresponder a los usuarios a la solución implantada.	
op.acc.3 Segregación de funciones y tareas	**B**	**M**	**A**	70%	30%	La solución implantada permite la segregación de funciones y tareas mediante la asignación de permisos a usuarios específicos y a grupos de usuarios. La solución implantada permite la gestión diferenciada de las tareas críticas por dos o más usuarios mediante flujos, restringiendo los accesos individuales. Se pueden lanzar notificaciones o alertas a un usuario Administrador. La solución considera la separación de funciones de operación, configuración, mantenimiento y auditoria; no permite accesos a entornos o capas no asociadas a un perfil de acceso.	Existirá un proceso interno documentado, relacionado con la segregación de funciones y tareas en el sistema de información de la organización cliente.	En la solución implantada se pueden definir los distintos usuarios y grupos de usuarios. Se gestiona la asignación de permisos mediante opciones de menú, asociación de roles a los usuarios o grupos, etc., lo que permite establecer a qué funcionalidades accede cada usuario. La solución dispone de opciones de consulta y listado de usuarios y grupos, junto a las funcionalidades permitidas.
Op.acc.4 Proceso de gestión de derechos de acceso	**TODAS**			30%	70%	La aplicación permite la asignación y el bloqueo o cancelación ágiles de accesos de usuario.	La organización cliente dispondrá de un proceso interno relacionado con las altas, modificaciones y bajas de los usuarios, asociado con los principios de mínima funcionalidad, necesidad de conocer y capacidad de autorizar (según la medida de seguridad org.4). Se dispondrá asimismo de un proceso periódico de revisión de cuentas de usuario, incluidas las de la solución implantada, en especial las que disponen de derechos de administración.	
op.acc.5 Mecanismos de autenticación (usuarios externos)	**B**	**M**	**A**	80%	20%	La solución permite establecer la robustez de las contraseñas según diferentes requisitos de seguridad, claramente especificados (acorde a la política de contraseñas de la organización cliente). La solución prevé emplear contraseñas de un solo uso (OTP) y/o mecanismos para implementar un doble factor de autenticación,	La organización cliente debe definir su política de comunicación de claves. Los usuarios deben confirmar la recepción de las credenciales y ser notificados de las condiciones de uso del servicio. Deben existir, asimismo, controles en el sistema para la autenticación, considerando diferentes niveles y factores de composición y vigencia.	Se puede asociar el proceso de altas al directorio activo del sistema. Si el sistema es de categoría media o superior y la solución implantada únicamente permite un factor de autenticación, o admite varios, pero de forma no simultánea, deberá apoyarse en un segundo factor existente en la red del cliente, o en

						o bien se apoya con otro factor proporcionado por la red de la organización cliente. Si se implanta en sistemas de categoría media, la solución registrará los accesos informando al usuario del último efectuado con su identidad.	La organización cliente debe establecer una política de contraseñas que incluya su robustez y su fecha de caducidad, dado que las contraseñas deben ser cambiadas periódicamente. Se incluirán otros factores de autenticación, cuando sea necesario según la categorización del sistema, para compensar y complementar los ofrecidos por la solución aportada por el proveedor.	una solución externa, de forma que ambos factores se complementen entre sí. La aplicación debe disponer de funcionalidades que permiten a la organización cliente parametrizar la calidad y complejidad de las contraseñas en base a la política que tenga definida, cubriendo: • Permite seleccionar el número mínimo de caracteres. • Tipología de los caracteres (alfanuméricos, mayúsculas / minúsculas, caracteres especiales). • Mantiene un histórico de contraseñas no permitiendo repetir las últimas empleadas. • Permite especificar la periodicidad para la caducidad de la clave. • Permite especificar caducidad de la contraseña por falta de uso en tras período determinado, directamente o apoyándose en LDAP. • Permite seleccionar el número de intentos fallidos antes de su bloqueo.
op.acc.6 Mecanismos de autenticación (usuarios de la organización)	**B**	**M**	**A**	80%	20%	La solución permite establecer la robustez de las contraseñas según diferentes requisitos de seguridad, claramente especificados (acorde a la política de contraseñas de la organización cliente). La solución prevé mecanismos para implementar un doble factor de autenticación, o bien se apoya con otro factor proporcionado por la red de la organización cliente.	La organización cliente debe definir su política de comunicación de claves. Los usuarios deben confirmar la recepción de las credenciales y ser notificados de las condiciones de uso del servicio. Deben existir, asimismo, controles en el sistema para la autenticación, considerando diferentes niveles y factores de composición y vigencia.	Se puede asociar el proceso de altas al directorio activo del sistema. Si el sistema es de categoría media o superior y la solución implantada únicamente permite un factor de autenticación, o admite varios, pero de forma no simultánea, deberá apoyarse en un segundo factor existente en la red del cliente, o en

				Si se implanta en sistemas de categoría media, la solución registrará los accesos informando al usuario del último efectuado con su identidad. Si se implanta en sistemas de categoría alta, la solución suspenderá las credenciales tras un período definido de no utilización.	La organización cliente debe establecer una política de contraseñas que incluya su robustez y su fecha de caducidad, dado que las contraseñas deben ser cambiadas periódicamente. Se incluirán otros factores de autenticación, cuando sea necesario según la categorización del sistema, para compensar y complementar los ofrecidos por la solución aportada por el proveedor.	una solución externa, de forma que ambos factores se complementen entre sí. La aplicación debe disponer de funcionalidades que permiten a la organización cliente parametrizar la calidad y complejidad de las contraseñas en base a la política que tenga definida, cubriendo: • Permite seleccionar el número mínimo de caracteres. • Tipología de los caracteres (alfanuméricos, mayúsculas / minúsculas, caracteres especiales). • Mantiene un histórico de contraseñas no permitiendo repetir las últimas empleadas. • Permite especificar la periodicidad para la caducidad de la clave. • Permite especificar caducidad de la contraseña por falta de uso en tras período determinado, directamente o apoyándose en LDAP. Permite seleccionar el número de intentos fallidos antes de su bloqueo.
op.exp.1 Inventario de activos	**TODAS**	50%	50%	El proveedor facilita toda la información relacionada con la solución implantada y, en su caso, el hardware específico necesario para la implantación que pudiera llegar a aportar, con miras a facilitar su inventariado por parte de la organización cliente. Sería una excelente buena práctica el incluir información sobe las librerías, módulos o complementos individuales empleados en el	La organización cliente mantendrá un inventario actualizado de todos los elementos del sistema, incluida la solución implantada, detallando su naturaleza e identificando a su responsable.	La organización cliente acordará con el proveedor el formato en que éste le entregará el inventario correspondiente a la solución, para facilitar su integración con el inventario corporativo.

					desarrollo de la solución, que deban conocerse por parte de la organización cliente.		
op.exp.2 Configuración de seguridad (bastionado)	**TODAS**			60%	40%	La solución permite cumplir los requerimientos de configuración segura: Asignación de las funcionalidades según necesidad, control de las funciones críticas y deshabilitación de las funciones no requeridas. Las acciones de los usuarios serán seguras salvo que el usuario actúe conscientemente. La solución dispone de la posibilidad de definir diferentes perfiles y niveles de seguridad. En la Guía de instalación el proveedor de la solución incluirá un apartado con las acciones de base de bastionado y aquellas que deban efectuarse con la colaboración del cliente.	Se retirarán las cuentas y contraseñas estándar y por defecto de la solución. Se recomienda eliminar las mismas en servidores y otros dispositivos conectados con la misma. Se atenderá a las consideraciones de bastionado presentes en la Guía de instalación proporcionada por el proveedor de la solución.	En determinados casos, el proveedor aporta una checklist de evaluación de la configuración segura de la solución.
op.exp.3 Gestión de la configuración de seguridad	**B**	**M**	**A**	50%	50%	El proveedor de la solución dispone de un procedimiento para garantizar la actualización de diagramas de estructura, inventario, documentación y guías de la solución, siempre que proceda, tras la implementación de un cambio.	La organización cliente dispondrá de un procedimiento para gestionar la configuración, en base a actualizaciones de diagramas, documentación, guías, etc., a partir de las diferentes soluciones aportadas externamente y los cambios que se vayan introduciendo en ellas.	Cada vez que se actualice el sistema operativo de la máquina, o máquinas, sobre las que se ejecuta la solución implantad, o se actualiza la versión del software que constituye dicha solución, deberá averiguarse si siguen siendo válidos los criterios de bastionado.
op.exp.4 Mantenimiento y actualizaciones de seguridad	**B**	**M**	**A**	80%	20%	El proveedor de la solución proporcionará periódicamente, y siempre que se requiera debido a su urgencia, avisos de vulnerabilidades, nuevos parches, versiones, cambios en la configuración, etc. Antes de publicar un parche, el proveedor ha realizado la batería de pruebas que se han considerado necesarias y lo ha notificado, y en su caso formado, a todo su personal de soporte a clientes.	La organización cliente dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones del fabricante de la solución y de otros fabricantes que soportan elementos del sistema. La organización cliente gestionará las garantías y contratos de mantenimiento. La organización cliente gestionará asimismo las licencias.	Se acordará entre proveedor de la solución y organización cliente un canal para reportar incidencias respecto a parches y actualizaciones instaladas, y para solicitarlos caso de no haberlos recibido.
op.exp.5 Gestión de cambios	**B**	**M**	**A**	80%	20%	El proveedor de la solución proporcionará toda la información necesaria a la organización cliente, para que ésta pueda analizar un cambio anunciado respecto a la solución implantada,	Especialmente para categoría media y alta, dispondrá de un procedimiento de Gestión de cambios que incluya registro, evaluación, aprobación, etc.	La organización cliente dispondrá de una herramienta para registrar las peticiones de cambio y que sirva de soporte para poder evaluarlas

						conociendo y evaluando los riesgos que implica antes de aprobarlo.	Interviniendo el responsable de Seguridad en aquellas peticiones de cambio que puedan implicar riesgo para la seguridad del sistema. La Gestión de Cambios de la organización cliente incluirá las peticiones de cambio con origen en los proveedores.	antes de su aprobación, manteniendo la trazabilidad de las mismas hasta su aprobación e implementación, o hasta su desestimación.
op.exp.6 Protección frente a código dañino	**B**	**M**	**A**	20%	80%	El proveedor garantiza que la solución podrá funcionar adecuadamente en el entorno del cliente junto con los principales softwares de control de código dañino existentes en el mercado. En determinadas ocasiones, se proporciona en la Guía de instalación una lista actualizada de los principales antivirus comerciales con los que ha sido probada la solución implantada.	La organización cliente dispondrá de mecanismos de protección frente a código dañino y seguirá las indicaciones de los fabricantes del mismo, cómo de los desarrolladores de otras aplicaciones en el sistema. Ante interferencias entre la solución implantada y el antivirus corporativo, puede solicitar ayuda al departamento de soporte del proveedor.	Cuando por cualquier circunstancia algún módulo de la solución implantada sea detectado como virus, se deberá gestionar la configuración del antivirus para declararlo como falso positivo, tras haberlo confirmado con el proveedor de la solución.
op.exp.7 Gestión de incidentes	**B**	**M**	**A**	80%	20%	El proveedor de la solución dispondrá de un procedimiento de gestión de incidentes conforme al ENS y las organizaciones cliente podrán hacer uso de un canal establecido al efecto para comunicar comportamientos anómalos o incidentes respecto a la solución implantada. El personal de soporte del proveedor asignará una categorización y escalado según la criticidad que perciba el cliente. Los registros de auditoría de la solución implantada permiten trazar la incidencia, bien mediante registros con origen en la propia solución o de los entornos que soportan la misma (servidor o directorio activo). Si la incidencia puede ser reiterativa en la solución, el proveedor informará con la mayor diligencia a todas las organizaciones cliente que dispongan de la misma versión y pudieran llegar a sufrir la misma incidencia y, según el nivel de	En la organización cliente se dispondrá de un procedimiento de gestión de incidentes que, en su caso, reaccione y aísle los servicios proporcionados por la solución en caso de necesidad, escalando el problema al proveedor de la solución. Se concienciará a los usuarios de la organización cliente para que comuniquen al Centro de Atención a los Usuarios (CAU) todas las incidencias sin dilación y siguiendo el procedimiento establecido.	Se acordará entre el proveedor de la solución y la organización cliente un canal para reportar incidentes de seguridad, como consecuencia del escalado de los mismos desde el CAU del cliente.

						riesgo, se apresurará en elaborar y distribuir un parche que la solucione.		
op.exp.8 Registro de la actividad de los usuarios	**B**	**M**	**A**	60%	40%	Existe un registro de actividad en la solución implantada que registra las acciones más importantes que realizan los usuarios. Dicho registro es configurable, dado que registrarlo todo podría significar elevados volúmenes de información. De forma genérica se registra toda la actividad referente a: • Segregación de funciones y tareas. • Gestión de derechos de acceso. • Mecanismos de autenticación. De forma específica se establece un campo que permite ser configurado por el cliente para indicar sobre que módulos o funcionalidades es necesario llevar a cabo un registro de la actividad de usuarios. Los registros reflejan en la medida de lo posible: • ¿Quién modifica? • ¿Qué se modifica? • ¿A quién afecta? • ¿Cuándo se modifica? El proveedor de la solución especificará claramente en la Guía de instalación dónde se almacenan los distintos LOGS (si no es parametrizable), con qué formato, cuando se borran, si están en claro o cifrados, etc. El proveedor de la solución habilitará un campo que permita configurar la ubicación donde se almacenaran dichos registros (preferiblemente en base de datos). Los eventos se registran en un formato estandarizado, comprensible para la mayoría de los correladores de eventos. Se especifica el período de retención y conservación de los LOGS, caso de no ser configurable.	Para categoría media, la organización cliente revisará los registros de actividad buscando patrones anormales, especialmente en horarios en que no se prevé se acceda a la solución. Para categoría alta, la organización cliente debe de llevar una gestión centralizada de todos los registros de LOGS generados por sus servicios, que le permitan realizar una correlación de los mismos (por ejemplo, con un SIEM) con el objeto de detectar actividades inusuales.	El proveedor de la solución debe proporcionar la información necesaria (ubicación de los LOGS proporcionados por la solución implantada, formatos, etc.) para que puedan así tratarse, preferiblemente de forma automatizada, estableciéndose las alertas adecuadas.

op.exp.9 Registro de Gestión de incidentes	**TODAS**			70%	30%	El proveedor de la solución implantada facilitará información respecto a la gestión de los incidentes al cliente. Para ello, dispone de un proceso documentado de la gestión para la gestión de incidentes, apoyado en una herramienta de registro y seguimiento. Dicho registro le permite al proveedor obtener estadísticas de tipología de incidentes acaecidos en la solución y poner medios para evitar su ocurrencia futura en relación a todos sus clientes.	Existirá en la organización cliente un proceso de control de las incidencias gestionadas internamente, incluyendo las derivadas al proveedor de la solución implantada, que permita verificar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS/SLA) respecto al soporte proporcionado.	
op.exp.10 Protección de las claves criptográficas	**B**	**M**	**A**	50%	50%	La solución permite el uso de elementos criptográficos certificados y acreditados. Las claves caducadas serán rechazadas.	Existirá un proceso de control de las claves criptográficas en todo su ciclo de vida.	Se emplearán gestores de claves para almacenar las contraseñas de administración del sistema y las claves criptográficas necesarias, incluyendo las requeridas por la solución. Si el gestor de claves es centralizado/compartido, se crearán grupos de perfiles para su gestión segura sin que todos quienes accedan dispongan de acceso global a todo el contenido.
op.ext.1 Contratación y acuerdos de nivel de servicio (SLA)	**B**	**M**	**A**	50%	50%	El proveedor de la solución suscribirá un acuerdo contractual con la organización cliente. Se detallará en él lo que se considera calidad mínima y comportamiento normalizado de la solución. El proveedor responderá ante comportamientos anómalos de la plataforma, mediante mantenimiento correctivo, especialmente el que corrija incidentes de seguridad. Como parte de dicho contrato, en una adenda al mismo, o en un documento aparte, se establecerán acuerdos de nivel de servicio (SLA). Los SLA al menos cubrirán las acciones de respuesta a incidentes reportados por la	En determinadas ocasiones la organización cliente se adscribe a unas condiciones generales de contratación, las cuales deben leerse detalladamente con antelación, en evitación de desagradables sorpresas futuras.	Se establecerán de forma clara las responsabilidades de las partes, proveedor y cliente, en relación a la solución aportada.

						organización cliente y frecuencia de elaborar y facilitar reportes de gestión.		
op.ext.2 Gestión diaria	**B**	**M**	**A**	70%	30%	El proveedor de la solución implantada facilitará información del servicio, como pueden ser los tiempos de respuesta respecto a los incidentes reportados y su comparativa con los SLA acordados. El proveedor facilitará los correspondientes canales para reportar incidentes y periódicamente informes de gestión respecto al departamento de soporte en lo que respecta al cliente contratante.	Existirá un procedimiento interno de evaluación de los proveedores, de los niveles de servicio y cumplimiento de los requisitos establecidos, más complejo como menor información facilite el proveedor.	Adicionalmente, pueden llegar a acordarse reuniones de seguimiento periódicas, aunque sea una vez al año, levantándose acta de las mismas y los acuerdos tomados.
op.ext.3 Protección de la cadena de suministro	**B**	**M**	**A**	20%	80%	En este ámbito no aplica inicialmente, salvo que el propio proveedor disponga de otro proveedor relevante para la solución implantada, por ejemplo, que se encargue de realizar el soporte de la misma. En ese caso se informará al cliente y se incluirá a dicho proveedor en el AA.RR. y en el BIA.	El cliente incluirá al proveedor de la solución implantada en modo local en el BIA y en su AA.RR., considerando que le proporciona soporte y/o mantenimiento correctivo y evolutivo.	
op.ext.4 Interconexión de sistemas	**B**	**M**	**A**	70%	30%	El proveedor de la solución implantada que le aporte soporte y/o mantenimiento de la misma, informará al cliente de las posibles interconexiones necesarias y solicitará autorización de las mismas.	El cliente, si procede, autorizará las interconexiones y documentará, como mínimo, las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.	Al menos para categoría alta, se establecerán mecanismos y procedimientos de coordinación entre ambas partes para la atribución de responsabilidades respecto a la operación de la interconexión.
op.nub.1 Protección de servicios en la nube	**B**	**M**	**A**			No aplica, al tratarse de una solución implantada en modo local y no proporcionada desde la nube.	No aplica en el ámbito del sistema de información implantado ON-PREMISE.	
op.cont.1 Análisis de impacto	**B**	**M**	**A**	60%	40%	El proveedor de la solución incluye el servicio de gestión de incidente, de soporte, y de mantenimiento correctivo a las organizaciones cliente en su análisis de impacto (BIA). También a sus proveedores relevantes para esos servicios.	La organización cliente incluirá en su análisis de impacto (BIA) y en el AA.RR. el soporte y mantenimiento a la solución aportada por el proveedor, así como quién los presta (averiguará del proveedor si hay subcontratación).	

						El proveedor de la solución facilitará toda la información requerida por el cliente para poder realizar sus propios análisis de impacto. El proveedor facilita un esquema de la arquitectura de la solución, para que la organización cliente conozca las dependencias de los elementos que son críticos para los servicios soportados por la solución.		
op.cont.2 Plan de continuidad	**B**	**M**	**A**	10%	90%	Si el proveedor dispone de un plan de continuidad que esté relacionado, directa o indirectamente, con la solución aportada o con servicios de soporte o mantenimiento correctivo, deberá informar al cliente.	El Plan de Continuidad deberá asegurar la solución, siempre que se haya determinado su conveniencia en el BIA. En caso afirmativo se conciliará la información aportada por el proveedor respecto a su Plan de Continuidad, con el propio Plan de Continuidad de la organización cliente.	
op.cont.3 Pruebas periódicas	**B**	**M**	**A**	10%	90%	El proveedor informará a la organización cliente de las pruebas realizadas respecto a su Plan de continuidad, y en qué fecha las ha realizado, con relación al soporte y mantenimiento correctivo de la solución aportada.	La organización cliente deberá realizar pruebas de su Plan de Continuidad, en relación a la solución implantada.	
op.cont.4 Medios alternativos	**B**	**M**	**A**	30%	70%	El proveedor informará al cliente si dispone de medios alternativos para proporcionar el servicio de soporte y el de mantenimiento correctivo.	El cliente se asegurará de que la solución implantada en modo local está redundada, a la vez que se interesará por la redundancia en el servicio de soporte y mantenimiento correctivo del proveedor.	
op.mon.1 Detección de intrusión	**B**	**M**	**A**	10%	90%	Inicialmente no aplica. No obstante, el proveedor dispondrá en su propia red de desarrollo, que posiblemente incluya a un repositorio de código fuente, de los mecanismos de detección y de prevención de intrusión necesarios para minimizar el riesgo de una alteración con fines maliciosos del código que se distribuirá posteriormente a los clientes.	La organización cliente dispondrá de herramientas específicas de detección y prevención de intrusión (IDS/IPS) o aprovechará dichas funcionalidades en los FW, caso de que dispongan de ellas, estén contratadas y configuradas.	
op.mon.2 Sistema de métricas	**B**	**M**	**A**	10%	90%	Para categoría media y alta el proveedor dispone de mediciones relacionadas con los incidentes que gestiona, que hayan sido abiertos por la organización cliente, incluyendo	La organización cliente calculará las métricas de categoría media, referidas a la gestión de incidentes, armonizándolas de ser necesario con las mediciones	

	B	M	A			los tiempos de resolución. Los empleará para facilitarle informes de cumplimiento de los SLA al cliente.	facilitadas por el proveedor de la solución respecto a los incidentes que le han sido escalados.	
op.mon.3 Vigilancia	B	M	A			El proveedor dispondrá de un sistema automático de recolección de eventos de seguridad, que a partir de categoría media permitirá la correlación de los mismos. Este sistema de monitorización será especialmente relevante mientas desarrolla y posteriormente se mantiene la solución.	El cliente dispondrá de un sistema automático de recolección de eventos de seguridad, que a partir de categoría media permitirá la correlación de los mismos, una vez se implante la solución en modo local sobre su infraestructura.	
mp.if.1 Áreas separadas con control de acceso	**TODAS**			10%	90%	Inicialmente no aplica. No obstante, el proveedor dispondrá de áreas separadas y protegidas donde se ubicará el repositorio de código fuente y el resto de la infraestructura TIC necesaria para poder prestar los servicios de soporte, mantenimiento y desarrollo.	La infraestructura TIC que soporta a la solución implantada, incluyendo los elementos hardware específicos que pueda incorporar, se instalará en áreas separadas protegidas con control de acceso.	
mp.if.2 Identificación de las personas	**TODAS**			20%	80%	Inicialmente no aplica. No obstante, el proveedor dispondrá de un sistema de identificación de las personas con acceso a la sala donde se encuentra el repositorio de código fuente. Únicamente personal autorizado e identificado debería acceder a la parametrización de la solución en el proceso de implantación en las dependencias de la organización cliente, bajo la supervisión del Responsable de Seguridad del mismo.	Se identificará a todas las personas que accedan a los locales donde se encuentran los equipos que soportan la solución y únicamente se permitirá trabajar en los equipos a personal cualificado que esté debidamente autorizado.	
mp.if.3 Acondicionamiento de los locales	**TODAS**			10%	90%	Inicialmente no aplica. No obstante, el proveedor dispondrá de sus dependencias acondicionadas para poder prestar los servicios asociados a la solución implantada (mantenimiento y soporte).	Se debe disponer de unas instalaciones auxiliares (CPD, sala técnica, etc.) adecuadas para garantizar el eficaz desempeño de la infraestructura TIC en la que se apoya la solución implantada, protegiéndola de los riesgos identificados.	
mp.if.4 Energía eléctrica	B	M	A	20%	80%	Inicialmente no aplica. No obstante, los elementos TIC necesarios para prestar servicios de soporte y atención al cliente tendrán garantizado el suministro eléctrico durante los	Debe garantizarse la energía eléctrica en los equipos que soportan la solución implantada y, en caso de fallo de suministro, garantizar su funcionamiento	

					tiempos acordados en los SLA suscritos con la organización cliente.	mediante SAIS y, a ser posible, generadores eléctricos.	
mp.if.5 Protección frente a incendios	**TODAS**			20%	80%	Inicialmente no aplica. No obstante, los elementos TIC necesarios para prestar servicios de soporte y atención al cliente tendrán garantizada la protección frente a incendios.	Deben protegerse frente a incendios los equipos que soportan la solución implantada, ya sean estos fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.	
mp.if.6 protección frente a inundaciones	**B**	**M**	**A**	20%	80%	Inicialmente no aplica. No obstante, los elementos TIC necesarios para prestar servicios de soporte y atención al cliente tendrán garantizada la protección frente a inundaciones.	Deben protegerse frente a incidentes causados por el agua, ya sean fortuitos o deliberados, los equipos que soportan la solución implantada.	
mp.if.7 Registro de entrada y salida de equipamiento	**TODAS**			10%	90%	No aplica. No obstante, el proveedor debe registrar la entrada y salida de equipamiento al área segura donde se encuentra la infraestructura TIC del proveedor de la solución empleada para poder dar servicio de mantenimiento y soporte, incluido el repositorio de código fuente.	En el área segura donde se ubica la infraestructura que soporta la solución implantada, existirá un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.	
mp.per.1 Caracterización del puesto de trabajo	**B**	**M**	**A**	50%	50%	El personal de desarrollo, mantenimiento y soporte del proveedor tendrán identificadas sus implicaciones respecto a la seguridad. Del mismo modo, el personal del proveedor asignado para implantar la solución en el cliente, cumplirá los requerimientos de seguridad establecidos por el propio cliente, además de los del proveedor.	Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Para el Sector Público, además de los que constan en la RPT se definirán los puestos sujetos a subcontratación, incidiendo en implicaciones de seguridad.	Se definirán perfiles y grupos de usuarios en la solución, acordes con los requisitos de seguridad.
mp.per.2 Deberes y obligaciones	**B**	**M**	**A**	50%	50%	En función de la funcionalidad de la solución implantada, se dispondrá de elementos que permitan al usuario conocer los derechos y obligaciones respecto al uso de la misma. En su defecto, se detallarán en el manual de usuario. El proveedor de la solución, especialmente su personal de soporte a clientes, suscribe cláusulas de confidencialidad.	Se informará a cada persona que trabaje en la solución implantada, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, ya sea personal interno o subcontratado.	Se suscribirán acuerdos de confidencialidad con los empleados. Se suscribirá un acuerdo de confidencialidad con el proveedor de la solución.
mp.per.3 Concienciación	**TODAS**			50%	50%	Todo el personal del proveedor de la solución, especialmente el de soporte directo al cliente, estará concienciado respecto a la	Se deben realizar las acciones necesarias para concienciar regularmente al personal.	

			confidencialidad y demás dimensiones de la seguridad.			
mp.per.4 Formación	**TODAS**	50%	50%	El proveedor de la solución puede desarrollar acciones formativas relacionadas con la misma, de manera que pueda conocerse por los usuarios las funcionalidades y acciones permitidas en la herramienta, así como su uso seguro. El personal de soporte del proveedor estará formado respecto al uso seguro de la solución implantada en el cliente, de modo que pueda asesorarle con conocimiento de causa.	Se formará regularmente al personal para el adecuado desempeño de sus funciones operando la solución, sobre la configuración de la misma a personal administrador, sobre la detección y reacción ante incidentes a los usuarios y al CAU y respecto a la correcta gestión de la información tratada por la plataforma a los usuarios. La referida formación se apoyará en el proveedor, al menos inicialmente.	
mp.eq.1 Puesto de trabajo despejado	**B** **M** **A**	O%	100%	No aplica.	Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Para categoría media o alta se guardarán bajo llave al abandonar el puesto.	
mp.eq.2 Bloqueo de puesto de trabajo	**B** **M** **A**	30%	70%	La aplicación puede disponer de un tiempo de inactividad de sesión, debiendo validarse de nuevo una vez alcanzado. Si la organización cliente establece la cancelación de las sesiones abiertas, habitualmente en accesos remotos a la solución, el proveedor habrá realizado el desarrollo previendo que esta casuística no altere o dañe la integridad de la base de datos.	En la organización cliente donde se haya implantado la solución, se dispondrá de políticas al efecto. Mediante directivas de dominio se establecerán los tiempos de inactividad del usuario antes de bloqueo del puesto, requiriéndose una nueva autenticación. Para categoría alta, las políticas de cancelación de sesiones inactivas pueden establecerse a nivel de directivas de dominio.	
mp.eq.3 Protección de dispositivos portátiles	**B** **M** **A**	0%	100%	No aplica. No obstante, si los desarrolladores o personal de mantenimiento y soporte del proveedor de la solución trabajan en remoto sobre equipos portátiles, se dispondrá de políticas y medidas de seguridad adecuadas, que incluyan el uso de VPN y tal vez cifrado del disco.	Los portátiles evitarán conectarse remotamente a la solución desde redes no seguras, especialmente sin emplear VPNs. Se evitará que el equipo contenga memorizadas claves de acceso remoto a la organización y/o a la solución.	

							Se dispondrá en la organización cliente de una política de trabajo remoto que se desarrollará con las medidas de seguridad oportunas.	
mp.eq.4 Otros dispositivos conectados a la red	**B**	**M**	**A**	50%	50%	El proveedor de la solución deberá tener en cuenta esta tipología de dispositivos especialmente en los entornos de desarrollo, y en aquellos desde dónde se da soporte a los clientes.	El cliente donde se implanta la solución deberá tenerlo en cuenta en el entorno productivo durante todo el ciclo de vida de la misma.	
mp.com.1 Perímetro seguro	**TODAS**			40%	60%	Cuando por motivo de la operativa y funcionalidad de la solución implantada pueda afectarse a este control del cliente abriendo determinados puertos y/o creando reglas específicas en el cortafuegos (FW), se informa claramente en la Guía de instalación de la solución implantada de todos los puntos necesarios para que la organización cliente pueda realizar en la configuración del FW, balanceadores, etc., los cambios necesarios para mantener la eficacia y compatibilidad de las funciones de seguridad del perímetro.	La organización cliente deberá disponer de un sistema cortafuegos que separe la red interna del exterior por el que atraviesen todos los flujos de información, debiendo estar autorizados previamente. Se deben estudiar con detenimiento las implicaciones de requerir crear nuevas reglas en el FW para la seguridad global del perímetro. Únicamente personal especializado y autorizado debe crear reglas en el FW, tras contrastar su necesidad y disponer de la pertinente autorización.	
mp.com.2 Protección de la confidencialidad	**B**	**M**	**A**	50%	50%	Cuando el proveedor de la solución requiera prestar soporte remoto, se establecerán VPN, temporales y controladas, que empleen algoritmos de cifrado acreditados y con alcance limitado. Se registrarán y verificarán los LOGS.	Se emplearán VPN para accesos desde el exterior del perímetro, siempre que la solución implantada no disponga de la suficiente seguridad propia (ser un portal Web).	
mp.com.3 Protección de la integridad y de la autenticidad	**B**	**M**	**A**	50%	50%	La solución implantada dispondrá de prevenciones frente a acciones de alteración de la información, ataques de inyección de código, o secuestros de sesión, especialmente si es accedida desde Internet. La solución solo permitirá como medios de autenticación los descritos en los controles de acceso. Los perfiles de usuario y sus derechos, si son gestionados por la propia solución, se almacenarán cifrados con la robustez adecuada.	Si la solución implantada ha de ser accesible desde el exterior sin VPN, se estudiará la posibilidad de implantar alguna solución tipo Web Application Firewall (WAF), en coordinación con el proveedor de la solución. Se realizará periódicamente algún test de intrusión, inicialmente y posteriormente cuando se introduzcan modificaciones significativas en la solución.	

mp.com.4 Separación de flujos de información en la red.	**B**	**M**	**A**	20%	80%	No aplica. No obstante, el proveedor de la solución proporciona en la Guía de instalación información sobre la arquitectura de la solución, junto a posibilidades y consideraciones ante posibles segregaciones.	Para categoría alta, se segregará la solución implantada de otras redes cuya coexistencia pueda entrañar riesgo para la seguridad global de la organización cliente. Se atenderá a las consideraciones del proveedor de la solución en la Guía de instalación.	
mp.si.1 Marcado de soportes	**B**	**M**	**A**	0%	100%	No aplica	Si se emplean soportes, debe existir una política de etiquetado en la organización cliente, que incluya los empleados para realizar backups de la solución implantada.	
mp.si.2 Criptografía	**B**	**M**	**A**	10%	90%	No aplica. No obstante, se recomendará al cliente, ya sea en acciones de soporte, o en la Guía de instalación y demás documentación de la solución, que cuando se realicen copias en soportes y elementos extraíbles se evalúe configurar su cifrado empleando algoritmos acreditados.	Debe existir una política de cifrado para soporte y medios removibles, al menos cuando salen de un área contrada. Se incluirán, especialmente para categoría alta, aquellos en los que pudieran externalizarse copias de seguridad, incluidas las de la solución implantada, considerando el riesgo y la calificación de la información almacenada.	
mp.si.3 Custodia	**TODAS**			0%	100%	No aplica.	Se custodiarán debidamente los soportes empleados (en cuanto a seguridad y condiciones ambientales), especialmente los que contengan las copias de seguridad de la solución implantada. Las copias de seguridad se conservarán en una ubicación distinta de la que contiene la base de datos copiada.	
mp.si.4 Transporte	**TODAS**			0%	100%	No aplica.	Se debe garantizar que los soportes y medios extraíbles, como pueden ser los que contienen las copias de seguridad, permanezcan bajo el control de la organización cliente y que satisfagan sus	

						requisitos de seguridad mientras están siendo desplazados. Se empleará un registro de entrada y salida, especialmente para transportes no recurrentes.	
mp.si.5 Borrado y destrucción	**B**	**M**	**A**	50%	50%	Se emplearán datos específicos de prueba. No obstante, cuando el personal de proveedor deba realizar acciones con datos del cliente, procurará anonimizarlos previamente. Si no fuera posible, se emplearán las mismas medidas de seguridad que en producción y al acabar se emplearán métodos de borrado seguro, conforme a productos certificados para categorías media y alta. Cuando se deban desinstalar versiones, o se proceda a retirar maquinas incluidas en la solución, se procederá a un borrado seguro y en su caso destrucción certificada con indicación individual del número de serie de los soportes destruidos.	La organización cliente dispondrá de una política de borrado y destrucción conforme a estándares acreditados. El responsable de seguridad de la organización cliente procederá a confirmar el proceso y el producto empleado para borrar o destruir los activos incluidos en la solución implantada, o que la soportan, antes de su retirada.	Se conservarán registros y evidencias del borrado y destrucción seguros.
mp.sw.1 Desarrollo	**B**	**M**	**A**	100%	0%	El proveedor de la solución empleará una metodología de desarrollo que tenga en cuenta la seguridad. No obstante, en desarrollos a medida se podrá emplear la metodología de la organización cliente. Se dispone de evidencias de control del desarrollo y de la calidad del mismo, así como de los datos de prueba empleados y cuáles de dichas pruebas son respecto a la seguridad. Se estará en condiciones de evidenciar la seguridad del proceso mediante diagramas u otros elementos en la Guía de instalación o demás documentación de la solución. La solución final implantada incluye requisitos de seguridad y, en concreto, elementos de identificación y autenticación, así como de protección de la información que trate.	Si la organización cliente dispone de una metodología de desarrollo que tenga en cuenta la seguridad, puede exigirse al proveedor de la solución que los desarrollos a medida se adapten a la misma. La organización cliente requerirá a los proveedores de la solución, habitualmente si es ésta a medida, el cumplimiento de un proceso de desarrollo en entorno separado al de producción.	

						La solución implantada incluirá registro de pistas de auditoría.		
mp.sw.2 Aceptación y puesta en servicio	**B**	**M**	**A**	70%	30%	El proveedor de la solución realiza análisis de vulnerabilidades y pruebas de penetración de la misma periódicamente, especialmente si se ha modificado la versión de la solución de forma relevante. Todo desarrollo para la solución, incluidas sus sucesivas versiones, evoluciones o parches, deberán haber sido comprobados antes de su lanzamiento con respecto a los requerimientos de seguridad en un entorno aislado y sin datos reales. El proveedor de la solución dará soporte a la organización cliente, si es requerido, con respecto a las pruebas de preproducción para evitar el deterioro de la seguridad.	La organización cliente requerirá al proveedor de la solución evidencias de la realización de análisis de vulnerabilidades. Para categoría media o alta, la organización cliente realizará pruebas de preproducción antes de la puesta en producción de la solución implantada, que se complementarán con un pentesting caso de ser una aplicación web. Se aconseja realizar un análisis de coherencia en la integración de la solución implantada con los sistemas existentes.	
mp.info.1	**TODAS**			50%	50%	El proveedor cumplirá con la legislación aplicable en materia de protección de datos. El proveedor colaborará con el Delegado de Protección de Datos (DPD) de la organización cliente (o con quién gestione dicha materia), para evidenciar el nivel de cumplimiento de la solución a la normativa. El proceso de desarrollo de la solución considerará la privacidad por defecto (PbD).	La organización cliente incluirá requerimientos de protección de datos en sus sistemas y para las soluciones externas que se contraten. Dispondrá de un DPD interno o externo (o de un responsable de la protección de datos) que supervisará el impacto o el riesgo que tiene la solución en el ámbito de la privacidad. Si lo estima necesario solicitará la realización de una EIPD. Contemplará la gestión del riesgo, incluyendo la privacidad, en la organización.	
mp.info.2 Calificación de la información	**B**	**M**	**A**	10%	90%	El proveedor de la solución mantendrá su propia normativa interna de calificación. La certificación del sistema de desarrollo, mantenimiento y soporte de la solución respecto al ENS, por parte del proveedor, determina el nivel de los servicios y datos a	Deberá disponerse en la organización cliente de una normativa interna de calificación de la información. Los activos de información deberán estar inventariados.	

						tratar por la solución una vez implantada en la organización cliente.		
mp.info.3 Firma electrónica	**B**	**M**	**A**	50%	50%	La solución implantada, de ser necesario, permitirá el empleo o la integración con otros servicios susceptibles de emplear firmas electrónicas ya sea para autenticación o para asegurar la integridad de la información gestionada.	Existirá una política de firma electrónica. Para categoría media y alta, se verificará que cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados. Para categoría alta, se instalarán los certificados de forma que se requiera un segundo factor del tipo «algo que se sabe» o «algo que se es. Se gestionarán los certificados, incluyendo el proveedor, las fechas de caducidad y las direcciones para el correo electrónico de aviso de renovación, a ser posible de forma centralizada.	
mp.info.4 Sellos de tiempo	**B**	**M**	**A**	50%	50%	De ser necesario en la solución implantada, se emplearán 'sellos cualificados de tiempo electrónicos'.	Si es de aplicación, e tendrán en cuenta los sellos de tiempo en la política de firma electrónica. De ser necesario para la solución implantada, ésta se basará en sellos de tiempo electrónicos cualificados. Se gestionarán los sellos de tiempo igual que se gestionan los certificados de firma electrónica.	
mp.info.5 Limpieza de documentos	**TODAS**			50%	50%	Este control puede ser cubierto por procedimientos y herramientas del cliente. No obstante, podría dotarse a la solución de mecanismos de control y borrado de determinados metadatos en los documentos generados y/o almacenados.	Se dispondrá de normativa interna referida al borrado de metadatos. Pueden implantarse soluciones internas, automáticas, o procedimientos manuales, que complementen o sustituyan a las prestaciones de la solución implantada. Debe recordarse que, en base al ENI, ciertos metadatos son requeridos a efectos de interoperabilidad, por lo que no siempre es aconsejable una eliminación indiscriminada.	

mp.info.6 Copias de seguridad	B	M	A	10%	90%	El proveedor realizará recomendaciones respecto a las copias de seguridad de la solución implantada en la Guía de instalación.	La organización cliente dispondrá de un procedimiento de copias en el que se configurarán las copias conforme a los RPO declarados en el BIA y siguiendo las recomendaciones del proveedor de la solución, especialmente para niveles medio y alto e disponibilidad. El proceso de copias debe incluir la información, aplicaciones, datos de configuración, etc. de la solución implantada. La organización cliente debe ser capaz de realizar una restauración completa en caso de evento disruptivo, con la ayuda del proveedor de la solución de ser necesario. Se deben planificar restauraciones de prueba, especialmente para nivel medio o alto en disponibilidad, planificadas en periodos adecuados, que permitan acreditar la integridad de las copias y del proceso.	
mp.s.1 Protección del correo electrónico	**TODAS**			50%	50%	Cuando una de las funcionalidades de la solución implantada sea el envío de notificaciones mediante correo electrónico, se dispondrá de un registro de actividades completo que incluya los correos electrónicos enviados. Se valorará la posibilidad de incluir funcionalidades antispam en relación al envío de correos electrónicos automáticos desde la solución, en base a permitir configurar: • Número de correos enviados por minuto. • Número de destinatarios que se pueden asignar en un solo correo. • Tamaño máximo del contenido del correo. • Establecer las posibles acciones a realizar si se intenta sobrepasar los parámetros	Debe existir en la organización cliente una política de correo electrónico y procedimientos de seguridad que incluyan los principales problemas de seguridad que suele tener asociados: cifrado de adjuntos sensibles, limitaciones de uso, etc., así como mecanismos de seguridad: antivirus en relación a correos entrantes y salientes y antispam. También se articulará la concienciación del usuario. Si la solución implantada no dispone de un servidor de correo electrónico propio, sino que se integra con el servidor de correo corporativo de la organización cliente a través	

					definidos, como cancelar el envío y enviar una notificación al usuario y/o al administrador.	del protocolo SMTP, será éste servidor el que se encargue de realizar la gestión requerida y deberá supervisarse.	
mp.s.2 Protección de servicios y aplicaciones web	**B**	**M**	**A**	50%	50%	A nivel del desarrollo de la solución, el proveedor ha tenido en cuenta la prevención de manipulación de URL, prevención de ataques de inyección de código, prevención de intentos de escalado de privilegios, de ataques "Cross site scripting", de ataques de manipulación de programas o dispositivos o de sistemas de almacenamiento, ya sea a nivel de las diferentes fases de desarrollo o bien en el propio ciclo de vida del producto una vez en producción. El proveedor establece auditorias de seguridad o hacking en sus productos para detectar vulnerabilidades, inicialmente y a cada nueva versión con cambios significativos. Se tienen en cuenta reglas que limiten el número de sesiones, tiempos de sesión o volumen de datos transferidos. Se siguen por defecto las recomendaciones Owasp para el desarrollo y se consideran las principales vulnerabilidades declaradas por el sector, habiéndose realizado un análisis de riesgos que se expone en la Guía de relación entre proveedor y cliente (Ver anexo II de ésta guía).	La organización cliente debe gestionar la seguridad en los servicios publicados mediante la solución implantada, incluyendo análisis de seguridad o hacking ético preferiblemente cada vez que el fabricante actualice la versión, realizándolo almenos una vez año. Se externalizan a terceros para lograr una separación entre quién gestiona y quién realiza las pruebas de penetración. Debe establecer una norma relacionada con las medidas de seguridad de los servidores y de la seguridad de las aplicaciones. Puede derivarse parte de la seguridad de los entornos publicados mediante Web Applications Firewall (WAF). Todas las aplicaciones web de la solución son comprobadas antes de ser puestas en producción y se verifica que se cumplen los criterios de aceptación en materia de seguridad y no se deteriora la seguridad de otros componentes del sistema, comprobándose las posibles vulnerabilidades según los principales estándares del sector.	
mp.s.3 Protección de la navegación web				30%	70%	No aplica directamente, aunque se considera un riesgo, por lo que se verificará, al menos, para el personal de desarrollo y de soporte de la solución.	Se verificará, al menos, para todo el personal que acceda a la solución implantada localmente.	
mp.s.4 Protección frente a la denegación de servicio	**B**	**M**	**A**	20%	80%	El proveedor ha dotado a la solución de funcionalidades mínimas para controlar: • Sesiones internas (concurrentes, abiertas). • Acciones fuera de los parámetros de seguridad interna del cliente (cancelar,	Se dispondrá de soluciones anti-DoS, ya sea implementadas como funcionalidades en el FW, mediante dispositivos especializados, o contratando servicios	

						bloquear, generar notificaciones y registros).	específicos al proveedor de comunicaciones. Se dimensionará el sistema con holgura, respecto a las tablas de dimensionamiento que proporciona el proveedor en la Guía de instalación. Para categoría alta se establecerán procedimientos de reacción a los ataques, que incluyan comunicación con el proveedor de comunicaciones.	

9. ANEXO II. Ejemplo para confeccionar el análisis de riesgos de la solución implantada

*NOTA: Se recuerda que el **valor del riesgo** puede calcularse en función de la probabilidad de que se materialicen los riesgos identificados (amenazas) y de su consecuencia (impacto). En esta tabla, únicamente* a modo de ejemplo, *se identifican algunos riesgos basados en el TOP 10 de OWASP (versión para desarrolladores) y algunos otros relevantes, plasmándose posibles acciones de mitigación por parte del proveedor (desarrollador) y del cliente que contrata la solución.*
Se recomienda al proveedor que personalice las acciones de mitigación, así como los riesgos identificados, para que abarquen al conjunto de la solución implantada y su integración con la infraestructura de la organización cliente.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
TOP 10 OWASP				
A01: Pérdida de control de acceso	Controles de acceso ausentes o mal aplicados. Ocurre cuando los mecanismos de control de acceso fallan, o son débiles, permitiendo a actores no autorizados acceder a recursos sensibles.	Exfiltración o manipulación de datos, al poder actuar los atacantes como usuarios o administradores. Puede incluir navegación por directorios, escalado de privilegios o ejecución de comandos maliciosos.	Implementar control de acceso restrictivo por defecto. Estudiar validar la autorización en cada capa. Realizar pruebas unitarias de control de acceso. Deben registrarse los errores de autenticación.	Con la excepción de los recursos publicados abiertamente, denegar por defecto. Aplicar segregación de redes y funciones. Revisar roles y permisos periódicamente. Auditar logs de acceso, preferiblemente de forma automatizada detectando, por ejemplo, errores de autenticación repetidos.
A02: Fallos criptográficos	Errores en uso o gestión del cifrado. Ocurre cuando se exponen datos sensibles debido a la falta de cifrado adecuado o el uso de algoritmos débiles, ya sea en tránsito o, si se requiere, en reposo.	Exposición de datos sensibles. Suplantación de identidad.	Emplear algoritmos de cifrado seguro y usar certificados actualizados. Realizar rotación de claves. Uso de bóvedas de secretos para almacenar claves API y/o certificados.	Configurar protocolos TLS de última versión, por ejemplo 1.3 (TLS fuerte) de las posibilidades disponibles en el sistema implantado. Mantener repositorios de certificados protegidos. Definir una política de cifrado en tránsito y en reposo.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
				Emplear gestores de contraseñas alineados con dicha política.
A03: Inyección	Entrada no validada al sistema que desencadena comandos no previstos desde ese origen. Ocurre cuando no se validan todos los campos de modo que se acepten únicamente los caracteres esperados.	Ejecución de código o comandos no deseados. Pérdida o corrupción de datos. En ocasiones se puede llegar al compromiso total del sistema.	Usar consultas parametrizadas. Validación estricta, especialmente en campos de entrada. Menor privilegio en la base de datos (BBDD). *NOTA: Estas fallas son fáciles de descubrir al examinar el código, pero difíciles de descubrir por medio de pruebas. En consecuencia, se recomienda que el desarrollador incorpore a su metodología análisis de código fuente.*	Segmentar la BBDD si es responsabilidad del cliente. Emplear herramientas de escaneo automatizadas (OWASP ZAP, Burp Suite, sqqlmap, etc.). Realizar pruebas de penetración, tal vez una combinación de pruebas manuales y herramientas automatizadas para evaluar a fondo la superficie de ataque de la solución y descubrir cualquier debilidad de inyección SQL u otra. Emplear y configurar un WAF en aplicaciones web. Monitorear el tráfico entrante, identificando patrones sospechosos y, como consecuencia, aplicar reglas predefinidas para mitigar los ataques de inyección. Mantener las soluciones actualizadas con los últimos parches de seguridad.
A04: Diseño inseguro	Fallos de diseño sin considerar las posibles amenazas. Ocurre cuando no se construye la solución en base a una metodología de diseño y desarrollo seguro.	Vulnerabilidades estructurales difíciles de corregir, con consecuencias imprevisibles.	Incorporar la seguridad desde el diseño (SbD) mediante modelado de amenazas, patrones de diseño seguro y arquitecturas robustas.	Solicitar revisiones de arquitectura. Exigir pruebas de seguridad previas a la implantación.
A05: Configuración de seguridad incorrecta	Configuraciones por defecto o inseguras. Ocurre cuando se producen errores en la configuración, como	Aumento de la superficie de exposición. Explotación de servicios.	Automatizar la configuración segura.	Bastionado de servidores, middleware y base de datos relacionados con la solución.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
	empleo de contraseñas predeterminadas, que dejan la solución implantada vulnerable.		Establecer plantillas de despliegue reforzadas (bastionadas).	Establecer procedimientos repetibles para configuraciones seguras. Auditorías periódicas de las configuraciones.
A06: Componentes vulnerables y desactualizados	Uso de componentes, módulos, librerías, con vulnerabilidades conocidas. Uso de dependencias de software no actualizadas que exponen las aplicaciones a vulnerabilidades conocidas. *NOTA: El vector de ataque tiene en cuenta lo fácil que resulta encontrar exploits para muchas vulnerabilidades conocidas.*	Compromiso del sistema al trabajar muchos componentes y módulos de software con todos los privilegios. Ejecución de código remoto.	Elaborar y mantener un inventario de componentes, módulos y librerías empleadas para el desarrollo (SBOM), así como sus dependencias en la solución desarrollada, gestionando versiones. Monitorear CVEs relacionados con los componentes empleados y actualizar o reemplazar los vulnerables.	Mantener inventario del software empleado en la solución, con el mayor nivel de granularidad. Exigir al proveedor el compromiso de elaborar y/o proporcionar sin dilación los parches de seguridad que solucionen las vulnerabilidades conocidas. Planificar ventanas de mantenimiento. *NOTA: Cada organización cliente debe asegurarse de que exista un plan continuo para monitorizar, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la solución implantada, coordinado con el proveedor.*
A07: Fallos de identificación y autenticación	Errores en autenticación o gestión de sesiones. Ocurre cuando se permite el empleo de contraseñas débiles, gestión inadecuada de sesiones o autenticación mal implementada, lo que facilita accesos no autorizados.	Secuestro de cuentas. Acceso no autorizado.	Implementar MFA. Almacenar contraseñas de forma segura. Tokens con expiración.	Imponer políticas de contraseñas (organizativas y técnicas). Aplicar autenticación centralizada y multifactor.
A08: Fallos de integridad de software y datos	Falta de verificación de la integridad del software o de los datos.	Compromiso del código fuente de las nuevas versiones o de los parches y actualizaciones intermedias.	Firmar los artefactos o aplicaciones resultantes del desarrollo de software.	Verificar la integridad de las entregas, que podrían contener puertas traseras.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
	NOTA: está vinculado con ataques a la cadena de suministro, actualizaciones comprometidas o el uso de componentes no confiables.		Validar la integridad del software. *NOTA: A menudo consistirá en proteger pipelines CI/CD (conjunto de pasos automatizados diseñados para optimizar el desarrollo, prueba e implementación de software, basado en prácticas de DevOps).*	Exigir firmas digitales al proveedor para garantizar que no han sido manipuladas las entregas, Controlar las fuentes (los orígenes) del software que se pretende instalar en el sistema de información.
A09: Fallos en el registro de logs y monitoreo de seguridad	Registro de logs o alertas insuficientes, dificultando la detección y respuesta a incidentes de seguridad. *NOTA: Los atacantes confían en la falta de monitorización y respuesta oportuna para lograr sus objetivos sin ser detectados.*	Detección tardía de incidentes. *NOTA: Los ataques de mayor éxito empiezan con el sondeo de vulnerabilidades. Permitir que tales sondas continúen actuando, al no ser detectadas, puede aumentar la probabilidad de una explotación exitosa casi al 100%.*	Deben registrarse todos los eventos relevantes, de forma que puedan establecerse alertas. Deben de realizarse pruebas de detección.	Centralizar registros de logs. Mantener un SIEM, o equivalente, local. Definir alertas y procedimientos de respuesta. Considerar emplear un WAF para souciones web.
A10: Falsificación de solicitud del lado del servidor (SSRF)	El 'atacante' fuerza al servidor de la solución a realizar peticiones controladas.	Acceso a redes internas. Fuga de datos. *NOTA: Estas vulnerabilidades permiten a un atacante manipular solicitudes enviadas por la aplicación a recursos internos, comprometiéndolos*.	Validación y Sanitización de Entradas de los usuarios antes de utilizarlas en cualquier solicitud HTTP. Utiliza listas blancas para permitir solo URLs y dominios seguros. Bloquear rangos internos restringiendo puertos y protocolos permitidos para las solicitudes salientes desde la aplicación. Bloquear el acceso a servicios que no sean necesarios. Protección de Información Sensible: Evitar mostrar mensajes	Filtrar el tráfico de salida. Segmentar redes. Configura correctamente la infraestructura de red mediante firewalls para bloquear el acceso desde el exterior a servicios internos.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
			de error detallados en caso de falla en las solicitudes SSRF, ya que esto podría revelar información sensible sobre la infraestructura interna.	
OTROS RIESGOS				
E01: Poca seguridad de las Interfaces de Programación de Aplicaciones (en inglés, APIs).	Riesgos específicos en APIs (autorización, inventario, consumo inseguro).	Acceso no autorizado o fuga de datos.	Implementar control de acceso por objeto. Aplicar limitación de velocidad (rate-limiting), es decir, establecer un mecanismo que controla la cantidad de solicitudes que se puede realizar a los puntos finales de la API dentro de un período de tiempo específico. Versionado y contratos estrictos.	Usar gateways. Realizar auditorías de las APIs. Revisar la exposición y la forma de autenticación.
E02: Compromiso de la cadena de suministro (especialmente en desarrollo)	Ataques a dependencias o pipelines de compilación.	Compromiso de desarrollos. Introducción de puertas traseras.	Controlar orígenes. Firmar dependencias. Validar desarrollos Mantener repositorios de código fuente asegurados.	Auditar proveedores o exigirles certificación del ENS con alcance que abarque el desarrollo. Exigir inventario de componentes (SBOM).
E03: Referencia directa a objetos.	Ocurre cuando un desarrollador expone una referencia a un objeto de implementación interna, tal como un fichero, directorio, o base de datos. Los atacantes pueden manipular estas referencias para acceder a datos no autorizados.	Comprometen toda la información que pueda ser referida por parámetros.	Deben evitarse referencias en claro a objetos de implementación interna. Efectuar análisis de código para mostrar rápidamente si las autorizaciones se verifican correctamente	No aplica.
E04: Falsificación de peticiones en	Ocurre cuando se permite al atacante forzar el navegador de la víctima para generar	Los atacantes pueden cambiar cualquier dato que a víctima esté autorizada a cambiar, o	Realizar un análisis de código para detectarlo.	Realizar pruebas de penetración para detectarlo.

Identificación de riesgos				
Riesgo	Descripción del riesgo	Impacto / Consecuencia	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
sitios cruzados (CSRF)	solicitudes que la aplicación vulnerable piensa que son peticiones legítimas que provienen de la víctima. La detección es bastante fácil a través de pruebas de penetración o de análisis del código.	acceder a cualquier funcionalidad donde esté autorizada, incluyendo el registro, cambio de estado o cierre de sesión.		
E05: Manejo incorrecto de errores	Algunas aplicaciones pueden filtrar involuntariamente información sobre su configuración y funcionamiento.	Acceso a datos de estado interno y conocimiento de vulnerabilidades por medio de mensajes de error.	Codificar los mensajes de error que proporciona la aplicación de manera que se minimice la información proporcionada en los mismos.	Únicamente el equipo de soporte del proveedor de la solución y el CAU de la organización cliente deben conocer el significado de los códigos de error.
E06: Integraciones GenAI / LLM	Riesgos derivados de integrar IA generativa en la solución.	Exfiltración o fuga de información sensible. Ejecución no controlada. Posibles ataques de inyección de prompt.	Validar entradas/salidas. Aislar integraciones. Aplicar filtros y límites.	Definir políticas de uso de IA en la organización. Mantener supervisión humana. Aislar datos sensibles de la IA.