centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 858

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

Junio 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-20-107-X

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.06.08 18:23:58 +02'00'

Fecha de Edición: junio de 2020

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

PRÓLOGO

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

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

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

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

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

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Junio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Se han cumplido más de diez años desde que se promulgara el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado posteriormente por el Real Decreto 951/2015. Posteriormente, se han promulgado cuatro (4) Instrucciones Técnicas de Seguridad (ITS) en base a Resoluciones de la Secretaría de Estado de Función Pública.

Asimismo, han transcurrido más de dos años desde que, con la participación de la Entidad Nacional de Acreditación (ENAC), se desarrollara el Esquema de Certificación del Esquema Nacional de Seguridad (ENS), referencial que ha servido para que, tras superar las preceptivas auditorías, hayan obtenido la Certificación de Conformidad con el ENS múltiples sistemas de información de entidades pertenecientes tanto al sector público como al privado.

El camino recorrido ha permitido detectar aspectos que han surgido de la constante evolución de los sistemas y del perfeccionamiento del propio Esquema de Certificación del ENS. Una de tales circunstancias se da cuando una organización contrata externamente un sistema, subsistema o solución integrante del mismo, que, pese a haber sido originariamente diseñada o/y explotada en la Nube (en modalidad SaaS, habitualmente), se implanta en la infraestructura tecnológica de la propia organización cliente, en modo local; lo que se conoce como *ON-PREMISE*.

Mientras que en las soluciones prestadas desde la Nube las medidas de seguridad corresponden casi en exclusiva al prestador del servicio, en las soluciones implantadas *ON-PREMISE* las medidas de seguridad se reparten entre ambos: proveedor que suministra y organización cliente que contrata.

El Anexo I de la presente Guía contiene una propuesta de reparto de la responsabilidad de implantar las correspondientes medidas de seguridad, que deberá acomodarse a cada caso en particular.

NOTA: Debe considerarse que el hecho de que un proveedor privado esté en posesión y pueda exhibir la correspondiente Certificación de Conformidad con el Esquema Nacional de Seguridad de los servicios soportados por su sistema de información, junto con el hecho de que cualquier organización del Sector Público realice un adecuada instalación de una solución externalizada conforme a las pautas de seguridad dadas por el proveedor, no eximirán en ningún caso a la misma de sus obligaciones con respecto al cumplimiento y adecuación del Real Decreto 3/2010 y por ello, conforme a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, obtener la correspondiente Declaración o Certificación de Conformidad acorde a la categoría de su sistema.

2. OBJETO

El objeto de esta Guía es desarrollar lo planteado, en primer lugar, en la Guía de Seguridad CCN-STIC "**CCN-CERT IC-01/19 ENS: Criterios adicionales de auditoría y**

certificación" y, posteriormente, en el *abstract* "**Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local**".

Cada proveedor de soluciones que haya de implantarse en la infraestructura tecnológica de su cliente en modo local (ON-PREMISE) deberá adaptar el contenido de este documento a su realidad concreta, considerando que ésta es la finalidad de las guías: permitir conocer la seguridad inherente en la solución aportada, posibilitando adaptarla y complementarla con la necesidad existente en cada organización cliente.

Por último, 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 otorgar 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 recogido en un único documento las tres (3) guías que se han considerado necesarias que el proveedor de la solución implantada en modalidad ON-PREMISE entregue a su cliente: la **Guía de instalación** (dirigida a administradores), la **Guía de uso seguro** (dirigida a usuarios) y la **Guía de relación entre proveedor y cliente**.

No obstante, forma parte de la responsabilidad del proveedor de la solución ON-PREMISE entregar a su cliente **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 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, al 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, 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.

Los epígrafes siguientes señalan los correlativos epígrafes de que debe disponer la precitada Guía.

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 deba conocer el 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 posible envío de e-mails 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 los servicios prestados, será responsabilidad del proveedor de la solución.

5.4 Dimensionamiento de la solución

Se proporcionará 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.
- 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 prestador/fabricante 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 integración del sistema

Se indicarán aquellas posibles pruebas de integración 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 integran de forma correcta sin interferencias funcionales ni menoscabo de la seguridad.

5.8 Requisitos de seguridad

Se detallarán aquellos aspectos de la infraestructura del cliente que resultan 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 firewall, etc.

Los requisitos se determinarán en función de la categoría de seguridad del sistema. Por ejemplo, para categoría ALTA podrá requerirse una cabina o un servidor físico con los discos cifrados, si no es la propia aplicación la que cifre los datos.

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, medidas compensatorias o complementarias de vigilancia.

5.10 Comunicación de incidencias y solicitud de soporte

Si el soporte a los usuarios del sistema lo realiza 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.

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.

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.

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, señalando 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 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 de aquel 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 suministre 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 realiza 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 aquellas acciones concretas 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 LA RELACIÓN ENTRE CLIENTE Y PROVEEDOR

Esta Guía contendrá recomendaciones para la gestión de la relación entre el proveedor de la solución y el cliente contratante, especificando la carga de responsabilidad 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 responsabilidad exclusiva de una parte, de la otra u ambas una vez instalada en modo local apoyándose en la infraestructura del cliente.

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 las medidas 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, documentación adicional disponible al respecto, buenas prácticas de uso seguro, etc.

El reparto de responsabilidades cliente-proveedor será fijado, en primera instancia, por el cliente, aunque podrá ser pactado por ambas partes, atendiendo a las especiales circunstancias que concurran en cada caso concreto. En cualquier caso, el reparto final acordado deberá estar determinado en 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.

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**	**Responsabilidad**		**Acciones necesarias para el proveedor**	**Acciones necesarias para el cliente**	**Notas de implantación**
		Proveedor	**Cliente**			
org.1 Política de Seguridad	**TODAS**	50%	50%	El proveedor dispone de una política de seguridad accesible para el cliente, por ejemplo, en la URL: https://www.proveedor.es/politica-de-seguridad, o se le ha dado a conocer por otro medio.	Existirá una política de seguridad aprobada por el órgano superior.	La Política de Seguridad del Proveedor es necesaria solo hasta que el sistema se implanta en la infraestructura del cliente. A partir de ese momento, la única Política de Seguridad es la del cliente (que habrá de contemplar la presencia de sistemas *on-premise* y redactar preceptos en consecuencia).
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 un 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.	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**	Sí	Sí	El proveedor dispone de una gestión propia de riesgos en la que ha considerado los procesos de desarrollo, implantación, mantenimiento y soporte de la solución (en el caso de que se haya subcontratado). 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 tener un análisis de riesgos actualizado.
op.pl.2 Arquitectura de seguridad	**B**	**M**	**A**	50%	50%	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	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	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.

						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.	instalación.	
op.pl.5 Componentes certificados	**B**	**M**	**A**	100%	0%	Para categoría alta, los componentes adicionales, proporcionados conjuntamente con la solución implantada, están certificados.	La organización cliente procurará que los componentes de la infraestructura TIC que interactúen con la solución implantada estén certificados.	
op.acc.1 Identificación	**TODAS**			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	**TODAS**			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).	

op.acc.5 Mecanismos de autentificación	B	M	A	60%	40%	Para que las contraseñas sean únicamente conocidas por el propio usuario, éstas se guardan cifradas en la solución implantada; Para las altas de usuarios gestionadas por personal de servicio, como el Centro de Atención al Usuario (CAU) de la organización cliente, se han previsto contraseñas de un solo uso que se generan de forma aleatoria y se remiten directamente al propio usuario (móvil o correo) sin ser estas conocidas por la persona del CAU que realiza la gestión, obligándose asimismo a su reemplazo en el primer acceso a la solución. 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). Según la categoría del sistema donde se integre la solución, se incluyen mecanismos para implementar un doble factor de autenticación, o bien se apoya con otro factor proporcionado por la red de la organización cliente. Para integrarse en sistemas de categoría alta, la solución admite que las credenciales se suspenderán tras un periodo definido de no utilización.	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. 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 dispondrá de un proceso periódico de revisión de cuentas de usuario, en especial las que disponen de derechos de administración. 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.	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 una solución externa, de forma que ambos factores se complementen entre sí. La aplicación dispone 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 Acceso local	B	M	A	80%	20%	La aplicación no revela información del usuario ante intentos de acceso (no conserva el nombre de usuario y menos la clave). Se limita el número de intentos permitidos de autenticación insatisfactoria. La solución registra tanto los intentos de autenticación con éxito como los fallidos. Así mismo, la solución informa a los usuarios de sus obligaciones una vez obtenido el acceso. Para cumplir con requisitos de categoría media, la solución informa al usuario del último acceso efectuado con su identidad.	Para sistemas de categoría alta, se estudiará en el FW o en el WAF la posibilidad de limitar el acceso desde lugares distintos de los que deba accederse (por ejemplo, determinados países), siempre que sea adecuado y posible, cuando como suele ocurrir, no lo prevea la solución implantada.	Para facilitar el soporte técnico, el sistema muestra por pantalla errores para la resolución de incidencias, siempre codificados, no mostrándose en ningún momento mensajes informativos detallados del error, o de su solución, ni del sistema operativo o la base de datos sobre la que está integrado, que puedan ser aprovechados por un atacante para detectar algunas vulnerabilidades. Dichos errores deben facilitarse al Centro de atención del Usuario (CAU) de la organización

						Para cumplir con requisitos de categoría alta, el acceso se puede limitar por horario y fechas.		cliente, quizá en la Guía de instalación (para administradores), para que puedan así determinar y resolver las incidencias reportadas.
op.acc.7 Acceso remoto	**B**	**M**	**A**	60%	40%	La solución se ha elaborado en base a metodologías de desarrollo seguro que impiden los ataques corrientes, del tipo inyección de código, alteración de URL, etc. Se relacionarán claramente los puertos que deban permanecer abiertos, junto a su justificación, en la Guía de instalación.	El acceso a la solución en remoto será mediante mecanismos de autenticación seguros como IPSec o a través de VPN. Se realizará un test de intrusión antes de poner la solución en producción, accesible desde Internet. Se verificarán los puertos abiertos necesarios para que funcione la solución y su influencia en otras soluciones que coexistan en el sistema. Se analizarán las implicaciones de las reglas necesarias en el FW en relación a las ya existentes y la seguridad global.	Se gestionarán y protegerán los certificados de servidores necesarios para establecer accesos remotos seguros.
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 que pudiera ser aportado para la instalación, con miras a facilitar su inventariado por parte de la organización cliente. Se incluye información sobe las librerías, módulos o complementos individuales empleados, que deban conocerse por parte de la organización cliente.	La organización cliente mantendrá un inventario actualizado de todos los elementos del sistema, 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.
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 los casos en los que no sea posible cumplir con recomendaciones de configuración de seguridad del proveedor, se elaborará un documento explicando el motivo por el que no se han podido implementar.	En determinados casos, el proveedor aporta una *checklist* de evaluación de la configuración segura de la solución.
op.exp.3 Gestión de la configuración	**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	La organización cliente dispondrá de un procedimiento para gestionar la configuración, en base a actualizaciones de diagramas, documentación, guías, etc., a partir de las	

					que proceda, tras la implementación de un cambio.	diferentes soluciones aportadas externamente y los cambios que se vayan introduciendo en ellas.	
op.exp.4 (Mantenimiento)	**TODAS**			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 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, conociendo y evaluando los riesgos que implica antes de aprobarlo.	Se dispondrá de un procedimiento de Gestión de cambios que incluya registro, evaluación, aprobación, etc. 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.	La organización cliente dispondrá de una herramienta para registrar las peticiones de cambio y que sirva de soporte para poder evaluarlas antes de su aprobación, manteniendo la trazabilidad de las mismas hasta su aprobación e implementación o su desestimación.
op.exp.6 Protección frente a código dañino	**TODAS**			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, 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	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.

						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 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 modifica? • ¿A quién afecta? • ¿Cuándo modifica?	Para categoría media, la organización cliente revisará informalmente los registros de actividad buscando patrones anormales. Para categoría alta, se empleará un SIEM o correlador de eventos para tratar los LOGS de modo que permita gestionar la seguridad de forma centralizada.	Para categoría alta, el proveedor de la solución debe proporcionar la información necesaria (ubicación, formatos, etc.) para que puedan tratarse adecuadamente de forma automatizada los diferentes LOGS proporcionados por la solución implantada y poder establecer así las alertas adecuadas.
op.exp.9 Registro de Gestión de incidentes	**B**	**M**	**A**	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 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 los registros de actividad	**B**	**M**	**A**	50%	50%	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 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 con el objeto de detectar actividades inusuales.	La organización cliente, caso de no haber sido previsto por el proveedor, debe establecer mecanismos para proteger la confidencialidad de los LOGS, su integridad y su disponibilidad, incluyéndolos en la política de *backup*.
op.exp.11 Protección de 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. Únicamente se emplearán elementos criptográficos certificados y acreditados.	Se emplearán gestores de claves para almacenar las contraseñas de administración del sistema y las claves criptográficas necesarias, incluyendo las requeridas por la solución. Admitirán 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 organización cliente y frecuencia de elaborar y facilitar reportes de gestión.	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.
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	Existirá un procedimiento interno de evaluación de los proveedores, de los niveles de servicio y cumplimiento de los requisitos establecidos,	Pueden llegar a acordarse reuniones de seguimiento periódicas, aunque sea una vez al año, levantándose acta de las mismas y los

						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.	más complejo como menor información facilite el proveedor.	acuerdos tomados.
op.ext.9 Medios alternativos	**B**	**M**	**A**	0%	100%	Inicialmente no aplica. Salvo que el propio proveedor en su Plan de Continuidad disponga de un proveedor alternativo para transferirle el servicio (por ejemplo, el soporte y mantenimiento de la solución aportada) no le afecta. En ese caso se comunicará su existencia, y preferiblemente sus datos, a la organización cliente.	Para sistemas de categoría alta se tendrá elegido, estudiado y, a ser posible, comprometido contractualmente, un proveedor alternativo para prestar el servicio con las mismas garantías de seguridad.	
op.cont.1 Análisis de impacto	**B**	**M**	**A**	60%	40%	El proveedor de la solución incluye el servicio de gestión de incidentes y de soporte a las organizaciones cliente en su análisis de impacto (BIA). 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.	La organización cliente dispondrá de un análisis de impacto (BIA) que incluya la solución aportada por el proveedor.	
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, deberá informar al cliente.	Para categoría alta, 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.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	La organización cliente dispondrá de herramientas específicas de detección y prevención de intrusión (IDS/IPS) o aprovechará	

		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.	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 el proveedor dispone de mediciones relacionadas con los incidentes que gestiona, que hayan sido abiertas por la organización cliente, incluyendo los tiempos de resolución.	La organización cliente calculará las métricas de categoría media, referidas a la gestión de incidentes, armonizándolas de ser necesario con las mediciones facilitadas por el proveedor de la solución respecto a los incidentes que le han sido escalados.	
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 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 tiempos acordados en los SLA suscritos con la organización cliente.	Debe garantizarse la energía eléctrica en los equipos que soportan la solución implantada y, en caso de fallo de suministro, garantizar su funcionamiento 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.if.9 Instalaciones alternativas	**B**	**M**	**A**	0%	100%	No aplica. No obstante, para categoría alta, se dispondrá de instalaciones alternativas que alberguen la infraestructura TIC necesaria para prestar servicios de mantenimiento y soporte.	Para sistemas de categoría alta, se garantizará la existencia y disponibilidad de instalaciones alternativas que soporten la solución implantada, para poder seguir operando en el caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.	
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	**TODAS**			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 trabajadores. 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 confidencialidad y demás dimensiones de la seguridad.	Se deben realizar las acciones necesarias para concienciar regularmente al personal.	
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	Se formará regularmente al personal para el adecuado desempeño de sus funciones operando la solución, sobre la configuración de	

					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.	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.per.9 Personal alternativo	**B**	**M**	**A**	50%	50%	Se garantizará la existencia y disponibilidad, en el proveedor de la solución, de varias personas que se puedan hacer cargo de las funciones de soporte y mantenimiento correctivo en caso de indisponibilidad del personal habitual.	Para categoría alta, se garantizará la existencia y disponibilidad de otras personas, en la organización cliente, que se puedan hacer cargo de las funciones de administración de la solución en caso de indisponibilidad del personal habitual.	El personal alternativo deberá estar sometido a las mismas garantías de seguridad que el personal habitual.
mp.eq.1 Puesto de trabajo despejado	**B**	**M**	**A**	*No	Sí	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 se guardarán bajo llave al abandonar el puesto.	Si el servicio suministrado por el proveedor incluye personal, también le resultaría de aplicación.
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.ep.3 Protección de equipos 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. 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.9 Medios alternativos	**B**	**M**	**A**	50%	50%	El proveedor de la solución mantendrá el soporte acordado y no se considerarán, salvo limitaciones en los niveles de servicio, fallos en la atención por no disponer de medios alternativos.	La organización cliente dispondrá de medios alternativos de tratamiento para soportar la solución, conforme a los tiempos establecidos en el análisis de impacto.	

mp.com.1 Perímetro seguro	**B**	**M**	**A**	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. Para categoría alta dispondrá de doble corona de *clusters* de FW, de diferentes fabricantes. 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.	
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). Para categoría alta, se verificará el cifrado de los datos tratados por la aplicación y, en su caso, se cifrará la base de datos en que se apoye o se albergará en una cabina de discos que cifre por hardware.	
mp.com.3 Protección de la autenticidad y la integridad	**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 aplicación 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, especialmente cuando se introduzcan modificaciones significativas en la solución.	
mp.com.4 Segregación de redes	**B**	**M**	**A**	0%	100%	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.com.9 Medios alternativos	**B**	**M**	**A**	0%	100%	No aplica. Salvo los medios de comunicación empleados por el proveedor para prestar soporte sobre la solución implantada, si esta es de categoría alta.	Para categoría alta, se garantizarán medios alternativos de comunicaciones para mantener el acceso a la solución, cuando éste se requiere desde el exterior del perímetro de la organización cliente.	

mp.si.1 Etiquetado	**TODAS**	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 elementos extraíbles se evalúe configurar su cifrado empleando algoritmos acreditados.	Debe existir una política de cifrado para medios removibles, incluidos aquellos en los que pudieran externalizarse copias de seguridad, incluidas las de la solución implantada, que considere el riesgo y la calificación de la información almacenada.	
mp.si.3 Custodia	**TODAS**	0%	100%	No aplica.	Se custodiarán debidamente los soportes empleados, 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 dispositivos portátiles y móviles junto a los soportes, como pueden ser los que contienen las copias de seguridad, permanezcan bajo el control de la organización cliente y que satisfacen sus requisitos de seguridad mientras están siendo desplazados.	
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. 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 emplea una metodología de desarrollo que tiene 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	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	

						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. La solución implantada incluye registro de pistas de auditoria.	ésta a medida, el cumplimiento de un proceso de desarrollo en entorno separado al de producción.	
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, la organización cliente realizará pruebas de penetración antes de la puesta en producción de la solución implantada. Para categoría alta se realizará un análisis de coherencia en la integración de la solución implantada con los sistemas existentes.	
mp.info.1	**TODAS**			*Sí	Sí	El proveedor cumple 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, para evidenciar el nivel de cumplimiento de la solución a la normativa. El proceso de desarrollo de la solución considerara 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 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.	Si el proveedor actúa como Encargado de Tratamiento, el reparto de responsabilidades se regirá por las exigencias de la legislación en materia de Protección de Datos (RGPD+LOPDGDD). En caso contrario, la responsabilidad será 100% del cliente.
mp.info.2 Calificación de la información	**B**	**M**	**A**	0%	100%	El proveedor de la solución mantendrá su propia política 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 tratar por la solución una vez implantada en la organización cliente.	Deberá disponerse en la organización cliente de una política de calificación de la información. Los activos de información deberán estar inventariados.	

mp.info.3 Cifrado	**B**	**M**	**A**	0%	100%	No aplica. No obstante, el proveedor podría incorporar mecanismos de cifrado a la solución implantada.	Para categoría alta, la información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Se emplearán sistemas de cifrado en las cabinas de discos si la solución implantada no incorpora mecanismos de cifrado por software.	
mp.info.4 Firma electrónica	**B**	**M**	**A**	10%	90%	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, se verificará que la solución implantada emplee sistemas de firma electrónica avanzada, basados en certificados cualificados. 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.	La firma electrónica es un servicio externo a cualquier sistema *on-premise*, por lo que la máxima responsabilidad recae sobre el cliente. El proveedor únicamente deberá garantizar la integración.
mp.info.5 Sellos de tiempo	**B**	**M**	**A**	10%	90%	Para categoría alta, de ser necesario por aplicar este control, la solución implantada se basa en sellos de tiempo electrónicos cualificados.	Si es de aplicación, e tendrán en cuenta los sellos de tiempo en la política de firma electrónica. Para categoría alta, de ser necesario, la solución implantada se basará en sellos de tiempo electrónicos cualificados. Se gestionarán los sellos de tiempo.	El sellado de tiempo, por sus propias características, es una función externa a cualquier sistema *on-premise*, por lo que la máxima responsabilidad recae sobre el cliente. El proveedor únicamente deberá garantizar la integración.
mp.info.6 Limpieza de documentos	**TODAS**			10%	90%	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 referida al borrado de metadatos. Pueden implantarse soluciones internas, automáticas, o procedimientos manuales, que complementen 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.	Los datos tratados son del cliente, por lo que la máxima responsabilidad recae sobre él. El proveedor deberá garantizar que ha suministrado las herramientas necesarias para que pueda llevarse a cabo.
mp.info.9 Copias de seguridad	**TODAS**			10%	90%	El proveedor de la solución realizará recomendaciones respecto a las copias de seguridad de la solución 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. 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, 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 definidos, como cancelar el envío y enviar una notificación al usuario y/o al administrador.	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 del protocolo SMTP, será este 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	La organización cliente debe gestionar la seguridad en los servicios publicados mediante la solución implantada, incluyendo análisis de seguridad o hacking ético al menos 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.	

						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).		
mp.s.8 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, bloquear, generar notificaciones y registros).	Se dispondrá de soluciones anti-DoS, ya sea implementadas como funcionalidades en el FW, mediante dispositivos especializados, o contratando servicios 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.	
mp.s.9 Medios alternativos	**B**	**M**	**A**	0%	100%	No aplica.	Para categoría alta se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios que presta la solución implantada, en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales.	

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 se identifican algunos riesgos basados en el TOP 10 de OWASP y algunos otros, y se plasman 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**	**Consecuencia (impacto)**	**Posible acción de mitigación del proveedor (desarrollador)**	**Posible acción de mitigación de la organización cliente**
OWASP A1: **Inyección**	Las fallas de inyección ocurren cuando un atacante puede enviar información no confiable a un intérprete de comandos. Estas fallas son muy comunes, particularmente en el código antiguo. Casi cualquier fuente de datos puede ser un vector de ataque de inyección: variables de entorno, parámetros, servicios web externos e internos y todo tipo de usuarios. Las vulnerabilidades de inyección a menudo se presentan en consultas SQL, LDAP, XPath o NoSQL, comandos del sistema operativo, analizadores XML, encabezados SMTP, etc.	Pérdida o corrupción de datos, pérdida de privilegios o negación de acceso. Algunas veces, una inyección puede llevar al compromiso total del servidor.	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. A nivel de desarrollo, la prevención de la inyección requiere mantener los datos separados de los comandos y consultas. Utilice la validación de entrada positiva o "lista blanca" en el lado del servidor. Esto no proporciona una protección completa ya que muchas aplicaciones requieren caracteres especiales, como áreas de texto o API para aplicaciones móviles. Use LIMIT y otros controles SQL dentro de las consultas para evitar la divulgación masiva de registros en caso de inyección SQL.	No aplica.
OWASP A2: Ruptura de la **autenticación**	Ocurre cuando un atacante es capaz de asumir la identidad de un usuario, comprometiendo así el acceso a las credenciales o tokens del mismo. Los atacantes tienen acceso a cientos de millones de combinaciones válidas de nombre de usuario y contraseña para rellenar credenciales, disponen de listas de cuentas administrativas predeterminadas, pueden intentar	Los atacantes únicamente tienen que obtener acceso a unas pocas cuentas, o solo a una cuenta con derechos de administrador, para estar en condiciones de comprometer el sistema. Dependiendo del dominio de la solución, puede tener importantes consecuencias.	Prever doble factor de autenticación. Los ID de sesión no deben estar en la URL, deben almacenarse de forma segura e invalidarse después de cerrar sesión, período de inactividad o tiempos máximos de vida.	Establecer una robusta política de contraseñas. Emplear doble factor de autenticación.

	ataques de fuerza bruta automatizada o mediante herramientas de ataque de diccionario. Los ataques de administración de sesión se entienden bien, particularmente si localizan tokens de sesión no vencidos.			
OWASP A3: **Exposición de datos sensibles**	En lugar de atacar directamente a la criptografía, el vector de ataque consiste en que los atacantes roban claves, ejecutan ataques tipo "man-in-the-middle" o roban datos de texto sin cifrar del servidor mientras están en tránsito o en la aplicación cliente del usuario como puede ser un navegador. Generalmente se requiere un ataque manual. Las bases de datos de contraseñas de las que los atacantes se hayan podido apropiar podrían ser objeto de ataques de fuerza bruta con ayuda de las unidades de procesamiento de gráficos (GPU).	La vulnerabilidad con frecuencia compromete la totalidad de los datos que deberían haber sido protegidos. Por lo general, esta información puede incluir datos de información identificativa personal (PII) que a menudo requieren protección según lo definido por el RGPD y demás legislación aplicable en materia de protección de datos.	Emplear una gestión de claves adecuada, almacenando las contraseñas utilizando funciones de hash robustas y adaptativas. Deshabilitar el almacenamiento en caché para las respuestas de las aplicaciones respecto a presentar consultas de la base de datos que contengan datos confidenciales.	Disponer de una política de calificación de la información. Clasificar los datos procesados, almacenados o transmitidos por la solución implantada en base a dicha política. De ellos identifique las categorías especiales de datos según el RGPD. Aplicar controles o medidas de seguridad según dicha clasificación. Cifrar todos los datos confidenciales en tránsito y también en reposo para categoría alta del sistema. En ese caso, asegúrese de contar con algoritmos, protocolos y claves estándar fuertes y actualizados. Verificar de forma independiente la efectividad de la parametrización y la configuración de seguridad en general de la solución implantada.
OWASP A4: **Entidades externas XML (XXE)**	Los atacantes pueden explotar los procesadores XML vulnerables (antiguos o mal configurados) si pueden cargar XML o incluir contenido hostil en un documento XML, explotando código vulnerable, dependencias o integraciones.	Estas vulnerabilidades se pueden usar para extraer datos, ejecutar una solicitud remota desde el servidor, escanear sistemas internos, realizar un ataque de denegación de servicio, etc.	Siempre que sea posible, deben emplearse formatos de datos poco complejos, evitando grandes series de datos confidenciales. Se deben parchear o actualizar todos los procesadores XML y bibliotecas en uso por las aplicaciones o en el sistema operativo subyacente. Deshabilitar la entidad externa XML y el procesamiento de DTD en todos los analizadores XML de la aplicación, según la hoja de OWASP "Prevención XXE", por ejemplo. Implemente la validación positiva "lista blanca", el filtrado o la desinfección de entrada en el lado del servidor para evitar datos hostiles dentro de los documentos, encabezados o nodos XML. Verifique que la funcionalidad de carga de archivos XML o XSL valida el XML entrante mediante la validación XSD o similar. Durante el desarrollo, la revisión manual del código fuente es la mejor alternativa en aplicaciones grandes y complejas con muchas integraciones.	Puede considerarse el uso de firewalls de aplicaciones web (WAF) para detectar, monitorear y bloquear ataques XXE.

OWASP A5: **Ruptura del control de acceso**	La explotación del control de acceso es una habilidad básica de los vectores de ataque. Las herramientas que realizan pruebas de seguridad estáticas (SAST) y dinámicas (DAST) pueden detectar la ausencia de control de acceso, pero no pueden verificar si es operativo cuando está presente. La eficacia del control de acceso únicamente es detectable usando medios de prueba manuales.	El impacto técnico es que los atacantes pueden actuar como usuarios o administradores, o usuarios con funciones privilegiadas que crean, acceden, actualizan o eliminan cualquier registro.	El control de acceso solo es efectivo si se aplica en el lado del servidor, o en una API del servidor, donde el atacante no puede modificar la verificación del control de acceso o los metadatos. Con la excepción de los recursos publicados abiertamente, denegar por defecto. En desarrollo, implementar mecanismos confiables y probados de control de acceso una vez y reutilizarlos en todas las aplicaciones, incluida la minimización del uso de Intercambio de Recursos de Origen Cruzado (CORS). Los controles de acceso del modelo deben exigir la propiedad del registro, en lugar de aceptar que el usuario puede crear, leer, actualizar o eliminar cualquier registro. Debe deshabilitarse la lista del directorio del servidor web y asegurarse de que los metadatos del archivo (por ejemplo, .git) y los archivos de respaldo no estén presentes en las raíces web. Deben registrarse los errores de autenticación, alertando a los administradores cuando sea apropiado (por ejemplo, ante errores repetidos) Debe limitarse la velocidad de la API y del acceso al controlador para minimizar el daño de las herramientas de ataque automatizado. Los JSON Web Token (JWT) (ver RFC-7519) deben invalidarse en el servidor después de cerrar la sesión. Los desarrolladores y/o el personal de control de calidad deben incluir pruebas de control de acceso funcional y pruebas de integración de la solución implantada.	
OWASP A6: **Configuración incorrecta de la seguridad**	Los atacantes a menudo intentarán explotar fallas no parcheadas o acceder a cuentas predeterminadas, páginas no utilizadas, archivos y directorios desprotegidos, etc. para obtener acceso o conocimiento no autorizado del sistema.	Tales vulnerabilidades frecuentemente dan a los atacantes acceso no autorizado a algunos datos del sistema o funcionalidad. Ocasionalmente, dichas vulnerabilidades resultan en un compromiso completo del sistema.	Los entornos de desarrollo, control de calidad y producción deben configurarse de manera idéntica, pero con diferentes credenciales utilizadas en cada entorno. En relación al desarrollo de la solución, una arquitectura de aplicación segmentada proporciona una separación efectiva y segura entre componentes o *tenants*, con segmentación, contenedores o grupos de seguridad en la nube (ACL).	Un proceso de bastionado sistemático que facilite la implementación de entornos protegidos adecuadamente. Las plataformas de la solución implantada deben estar minimizadas, sin características, componentes y documentación innecesarias. Del mismo modo deben eliminarse, o no instalarse, funcionalidades y *frameworks* no utilizados. Debe disponerse de un procedimiento para revisar y actualizar las configuraciones apropiadas conforme a todas las notas de

				seguridad, actualizaciones y parches, como parte del proceso de administración de parches.
OWASP A7: **Cross-Site Scripting (XSS)**	Ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. Permite a los atacantes ejecutar secuencias de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de los usuarios, destruir sitios web o dirigir al usuario a un sitio malicioso. Existen marcos de explotación de estas vulnerabilidades disponibles de forma gratuita.	El impacto de XSS es moderado para XSS reflejado y DOM, y severo para XSS almacenado, con ejecución remota de código en el navegador de la víctima, lo que permite robar credenciales, sesiones o entregar malware a la víctima.	Estas vulnerabilidades son detectadas de forma relativamente fácil a través de pruebas o por medio de análisis del código. La prevención de XSS requiere la separación de datos no confiables del contenido activo del navegador. Esto se puede lograr empleando *frameworks* que escapan automáticamente a XSS por diseño. Es imperativo conocer las limitaciones de la protección XSS de cada *framework* y maneje adecuadamente los casos de uso que no están cubiertos. Emplear técnicas de escape de datos en las solicitudes HTTP no confiables, basadas en el contexto en la salida HTML (cuerpo, atributo, JavaScript, CSS o URL) resolverán las vulnerabilidades XSS reflejadas y almacenadas. La hoja de OWASP "Prevención XSS" tiene detalles sobre las técnicas de escape de datos necesarias. La aplicación de codificación sensible al contexto al modificar el documento del navegador en el lado del cliente actúa contra DOM XSS. Cuando esto no se puede evitar, se pueden aplicar técnicas de escape sensibles al contexto similares a las API del navegador como se describe en la hoja de OWASP "Prevención XSS basada en DOM".	
OWASP A8: **Deserialización insegura**	Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques.	El impacto de explotar las vulnerabilidades de deserialización puede conducir a ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización puede conducir a la ejecución remota de código en el servidor.	Implementar verificaciones de integridad tales como firmas digitales en cualquier objeto serializado para evitar la creación de objetos hostiles o la manipulación de datos. Hacer cumplir estrictas restricciones de tipo durante la deserialización, antes de la creación de objetos, ya que el código generalmente espera un conjunto definible de clases. Se han demostrado derivaciones a esta técnica, por lo que no es aconsejable depender únicamente de esto. Aislar y ejecutar código que se desrealiza en entornos de bajos privilegios cuando es posible.	Registrar excepciones y errores detectados de deserialización, como cuando el tipo entrante no es el tipo esperado, o la deserialización presenta excepciones. También generar alertas si un usuario concreto deserializa constantemente. Restringir la conectividad de red entrante y saliente desde contenedores o servidores que deserializan, monitorizando el proceso.
OWASP A9: **Empleo de componentes con vulnerabilidades**	El vector de ataque tiene en cuenta que, si bien es fácil encontrar *exploits* para muchas vulnerabilidades conocidas, otras vulnerabilidades requieren un esfuerzo	Algunos componentes tales como librerías, *frameworks* y otros módulos de software casi siempre funcionan con todos los privilegios. Si e ataca un	Supervisar continuamente las fuentes como CVE y NVD para detectar vulnerabilidades en los componentes. Emplear herramientas de análisis de composición de software para automatizar el proceso.	Debe haber un proceso de administración de parches para eliminar dependencias no utilizadas, características innecesarias, componentes, archivos y documentación.

conocidas	concentrado para desarrollar un *exploit* personalizado.	componente vulnerable esto podría facilitar la intrusión en el servidor o una perdida seria de datos.	Suscribirse a las alertas por correo electrónico para conocer las vulnerabilidades de seguridad relacionadas con los componentes que se utilizan. Únicamente obtener componentes de fuentes oficiales a través de enlaces seguros. Preferiblemente paquetes firmados para reducir la posibilidad de incluir un componente modificado y malicioso. Supervisar las bibliotecas y los componentes que no están mantenidos o que no crean parches de seguridad para versiones anteriores.	Realizar un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, *frameworks*, bibliotecas) y sus dependencias. Si no es posible aplicar parches, considere implementar un parche virtual para monitorizar, detectar o proteger contra el problema descubierto. 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.
OWASP A10: **Insuficiente registro y monitorización**	La explotación insuficiente de LOGS y la monitorización insuficiente, son la base de casi todos los incidentes importantes. Los atacantes confían en la falta de monitorización y respuesta oportuna para lograr sus objetivos sin ser detectados.	Los ataques de mayor éxito empiezan con el sondeo de vulnerabilidades. Permitir que tales sondas continúen actuando puede aumentar la probabilidad de una explotación exitosa casi al 100%.	Asegurarse de que todos los errores de inicio de sesión, control de acceso y validación de entrada del lado del servidor puedan registrarse con suficiente contexto de usuario para identificar cuentas sospechosas o maliciosas, y conservarse durante el tiempo suficiente para permitir un análisis forense diferido. Asegurarse de que los registros se generen en un formato que las herramientas de correlación centralizadas puedan tratarlo fácilmente. Asegurarse de que las transacciones de alto valor tengan una pista de auditoría con controles de integridad para evitar alteraciones o supresiones, como pueden ser tablas de bases de datos de solo agregar o similares.	Establecer monitorización y alertas efectivas de manera que las actividades sospechosas se detecten y respondan de manera oportuna. Establecer o adoptar un plan de respuesta y recuperación de incidentes. Emplear firewalls de aplicaciones web (WAF).

Otros Riesgos

Riesgo	Descripción del riesgo	Consecuencia (impacto)	Posible acción de mitigación del proveedor (desarrollador)	Posible acción de mitigación de la organización cliente
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.
Ausencia de control de acceso a funciones	Este vector de ataque se da cuando no se verifica el control de accesos en el servidor al acceder a cada una de las	Permiten el acceso no autorizado de los atacantes a funciones del sistema. Las funciones	Las aplicaciones necesitan verificar el control de accesos en el servidor cuando se accede a cada una de sus funciones.	No aplica.

	funciones. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización adecuada accediendo a la función directamente.	administrativas son un objetivo clave de este tipo de ataques		
Falsificación de peticiones en sitios cruzados (CSRF)	Permite al atacante forzar al navegador de la víctima para generar 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.	Los atacantes pueden cambiar cualquier dato que la víctima está autorizada a cambiar, o acceder cualquier funcionalidad donde esté autorizada, incluyendo registro, cambio de estado o cierre de sesión.	Realizar análisis de código para detectarlo.	Realizar pruebas de penetración para detectarlo.
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.