BANCO DE **ESPAÑA**
Eurosistema

Dirección General de Servicios

Marzo de 2017

Gestión del patrimonio histórico-artístico del Banco de España. Requisitos de seguridad

Requisitos de Seguridad

Sistemas de Información

Hoja de Control

Título	Gestión del patrimonio histórico-artístico del Banco de España. Requisitos de seguridad
Autor	Sistemas de Información
Versión	1.0
Fecha	Febrero de 2017

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	08/02/2017	Primera versión

ÍNDICE

1 Introducción

Este documento describe los requisitos de seguridad a tener en cuenta en la contratación e implementación de un software de gestión del patrimonio histórico-artístico del Banco de España basada en una solución en la nube en modalidad Software as a Service (SaaS), así como las prescripciones técnicas aplicables a algunos de los controles de seguridad que se habrán de implementar.

2 Requisitos de seguridad

Este apartado describe los requisitos de seguridad de la información para el sistema de gestión del patrimonio. La determinación de dichos requisitos se deriva de las siguientes acciones:

- La valoración de la criticidad realizada por el Banco de España en términos de impacto para el negocio, financiero y reputacional en caso de la materialización de amenazas que pongan en riesgo la confidencialidad, integridad y disponibilidad del sistema.
- La identificación de las posibles amenazas a las que sería vulnerable un sistema de gestión del patrimonio, especialmente teniendo en cuenta la ubicación de dicho servicio en una nube accesible desde Internet.
- El catálogo de controles de seguridad propuesto por el estándar ISO/IEC 27002:2013, así como las recomendaciones incluidas en los estándares ISO/IEC 27017:2015 e ISO/IEC 27018:2014, sobre controles de seguridad y buenas prácticas para la gestión de datos personales para servicios en la nube.

2.1 Políticas de seguridad de la información

Para facilitar la comprensión de los controles que se especifican a continuación, cuando se indique «El Cliente» se hace referencia al «Cliente del Servicio en la Nube» y en concreto al «Banco de España», cuando se indique «Clientes» se hace referencia a «Los Clientes del Servicio en la Nube, además del Banco de España» y cuando se indique «El Proveedor» se hace referencia al «Proveedor del Servicio en la Nube».

ID	**SEG-1**
Nº control	27002-5.1.1/27017-6.3.1
Nombre	Políticas para la seguridad de la información y funciones y responsabilidades compartidas dentro de un entorno de nube.
Descripción	El proveedor ha de tener definido un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes. Así mismo las responsabilidades de las funciones compartidas de la seguridad de la información en el uso del servicio en la nube deben ser asignadas a figuras identificadas, documentadas y comunicadas por el proveedor.

Requisitos	Las políticas de seguridad definidas por el proveedor han de incluir al menos los siguientes aspectos: - Requisitos básicos de seguridad aplicables al diseño e implementación del servicio de la nube. - Acceso a los activos del cliente por parte del personal del proveedor, incluyendo procedimientos de control de acceso de los administradores. - Aislamiento de cada uno de los clientes, incluyendo detalles del sistema de virtualización. - Aseguramiento de la continuidad del negocio y recuperación ante desastres, incluyendo información sobre la política de backup. - Comunicación al cliente de la gestión de cambios. - Comunicación al cliente de posibles incidentes y brechas de seguridad. - Requisitos de seguridad aplicables a los datos de carácter personal. El proveedor debe documentar y comunicar sus capacidades, funciones y responsabilidades de seguridad de la información para el uso de su servicio, junto con los roles y responsabilidades que el cliente necesitaría implementar y administrar como parte de su uso.

ID	**SEG-2**
Nº control	27002-18.2.2
Nombre	Cumplimiento de las políticas y normas de seguridad
Descripción	El proveedor debe comprobar periódicamente el cumplimiento de las políticas de seguridad, las normas y otros requisitos de seguridad.
Requisitos	Se deben identificar y revisar los requisitos de seguridad definidos en las políticas, y asegurar que se cumpla la normativa aplicable. Si se encuentra cualquier incumplimiento como resultado de la revisión, se deberá: - Determinar la causa del incumplimiento. - Evaluar la necesidad de adoptar medidas para lograr el cumplimiento. - Aplicar las medidas correctivas apropiadas. - Revisar las acciones correctivas tomadas para verificar su eficacia y determinar las deficiencias o debilidades. Los resultados del examen y las acciones correctivas llevadas a cabo por el proveedor deben ser registrados y estos registros mantenidos en el tiempo, así mismo la revisión de seguridad como las medidas correctivas deberán ser reportados a un revisor independiente para su valoración.

2.2 Gestión de activos

ID	**SEG-3**

Nº control	27002-8.1.4/27017-8.1.5
Nombre	Devolución de activos y eliminación de los activos del cliente
Descripción	Todos los empleados y terceras partes deberán devolver y/ o devolverse todos los activos de la organización en el momento de la finalización del empleo, contrato o acuerdo.
Requisitos	En el momento de la finalización del contrato el proveedor deberá devolver al cliente los activos de información que estén en su posesión: - Se deberá devolver toda la información perteneciente al cliente: información de usuarios dados de alta, junto a sus autorizaciones, e información introducida en el sistema, registros de auditoría, etc. Esta información se deberá entregar en un formato que facilite su transferencia a otro proveedor. - Una vez realizada la entrega de los activos, el proveedor deberá realizar una destrucción segura de la información propiedad del cliente. - El proveedor debe proporcionar información sobre la devolución y eliminación de los activos del cliente al finalizar el acuerdo para su uso. - La devolución y remoción de activos deben estar documentados en el acuerdo. Estos deben especificar los activos que deben devolverse y eliminarse.

2.3 Control de acceso

ID	**SEG-4**
Nº control	27002-9.2.1
Nombre	Gestión de altas y bajas de cuentas de usuario
Descripción	Se debe establecer un proceso formal de registro y des-registro de usuarios, en caso de que estos no se realicen automáticamente, como paso previo al alta del usuario y la posterior asignación de derechos de acceso. En el caso del des-registro se procedería a la eliminación de los derechos de acceso y posteriormente a la baja del usuario.
Requisitos	El proveedor debe proporcionar funcionalidades de creación y baja de cuentas de usuario de forma que: - A cada usuario le sea asignado un identificador único, evitándose el uso de usuarios compartidos. - Dicha gestión de usuarios ha de poder delegarse a administradores de usuarios internos del cliente, quienes habrán de poder crear cuentas de usuarios, revisar las existentes, y borrar las que ya no sean necesarias.

ID	**SEG-5**
Nº control	27002-9.2.2

Nombre	Gestión de los derechos de acceso asignados a usuarios
Descripción	Se debe establecer un proceso formal de asignación y des-asignación de derechos de acceso de usuario a las distintas funcionalidades ofrecidas por el servicio en la nube.
Requisitos	El proveedor debe proporcionar funcionalidades de asignación y des-asignación de derechos de acceso basados en roles para todas las funcionalidades del sistema: - Ha de ser posible la designación de las funcionalidades disponibles para cada uno de los roles del sistema y dicha designación se ha de poder delegar en administradores internos del cliente. - La gestión de autorizaciones de la cuentas de usuario a cada uno de los roles se ha de poder delegar en administradores internos del cliente. - Se ha de poder obtener información de forma sencilla (por ejemplo, mediante la generación de informes) sobre las autorizaciones que cada usuario tiene asignada para facilitar la revisión periódica.

ID	**SEG-6**
Nº control	27002-9.2.3
Nombre	Gestión de los derechos de acceso con privilegios especiales
Descripción	La asignación y uso de derechos de acceso con privilegios especiales ha de estar restringida y controlada.
Requisitos	Tanto el proveedor como el integrador de la solución del cliente deben garantizar que la asignación de los privilegios de acceso como operador o administrador del sistema se realiza siguiendo las siguientes pautas: - Mediante un proceso de autorización formal que siga el principio de «necesidad de conocer» y durante el tiempo estrictamente necesario para la realización de las funciones de administración correspondientes. - Los accesos con privilegios especiales han de quedar auditados. - Cuando los administradores del sistema accedan utilizando privilegios especiales deberán autenticarse utilizando un mecanismo de autenticación de múltiples factores.

ID	**SEG-7**
Nº control	27002-9.2.4
Nombre	Gestión de la información confidencial de autenticación de usuarios

Descripción	La entrega de credenciales de acceso a los usuarios, en caso de que esta no se realice automáticamente, se ha de llevar a cabo mediante un proceso de gestión formal.
Requisitos	El proveedor debe garantizar que la entrega de credenciales a su usuario se realiza mediante un proceso formal en el que únicamente el usuario interesado, del que se ha verificado previamente su identidad, recibe las credenciales iniciales mediante un canal seguro, y que se ha de forzar la modificación de la contraseña inicial.

ID	**SEG-8**
Nº control	27002-9.4.2
Nombre	Proceso de inicio de sesión seguro
Descripción	El acceso al sistema se ha de realizar mediante un proceso de inicio de sesión seguro.
Requisitos	Para los accesos de usuarios internos del cliente, el proveedor deberá ofrecer la posibilidad de delegar la autenticación a un mecanismo interno del cliente. Para los accesos de usuarios internos del cliente, el acceso al sistema deberá estar basado en un doble factor de autenticación. Para la integración con las aplicaciones internas del cliente, la autenticación de las aplicaciones en ambas direcciones se basará en un mecanismo de autenticación suficientemente robusto. Para mayor información, consultar los requerimientos técnicos descritos en el apartado 3.

ID	**SEG-9**
Nº control	27002-9.4.3
Nombre	Gestión de contraseñas
Descripción	El sistema de gestión de contraseñas deberá ser interactivo y deberá asegurar la calidad de las contraseñas.
Requisitos	Los códigos de usuario y contraseñas que pudieran manejarse para la operación del sistema de gestión del patrimonio deberán ser individuales para mantener la auditoría del usuario que ha realizado una determinada acción. El sistema ha de ofrecer al usuario una opción para el cambio de contraseña y para su reinicio en caso de olvido. Se ha de forzar al usuario el cambio periódico de contraseña.

	Se ha de forzar al usuario a elegir una contraseña de calidad, incluyendo un mínimo de 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales. Se ha de mantener un histórico de las últimas contraseñas utilizadas para evitar su reutilización.

2.4 Criptografía

ID	**SEG-10**
Nº control	27002-10.1.1
Nombre	Política sobre el uso de controles criptográficos
Descripción	El proveedor ha de desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.
Requisitos	Los controles criptográficos que se implementen han de asegurar la confidencialidad e integridad de la información gestionada por el sistema sea aplicable tanto a los datos en tránsito (es decir, intercambiados entre el cliente y la nube, tanto en los accesos de usuarios personales como en los de las aplicaciones internas del cliente) como en reposo, (es decir, una vez almacenado en la base de datos y sistema de almacenamiento del proveedor).

2.5 Seguridad operacional

ID	**SEG-11**
Nº control	27017-12.1.5
Nombre	Seguridad operacional del administrador
Descripción	Los procedimientos para las operaciones administrativas de un entorno de nube deben ser definidos, documentados y monitorizados.
Requisitos	El proveedor debe proporcionar documentación sobre las operaciones y procedimientos críticos al cliente cuando este lo requiera.

ID	**SEG-12**
Nº control	27017-12.4.5
Nombre	Supervisión de servicios en la nube

Descripción	El cliente debe tener la capacidad de supervisar aspectos específicos de la operación de los servicios en la nube que utiliza.
Requisitos	El proveedor en la nube debe proporcionar capacidades que permitan al cliente supervisar aspectos específicos de la operación de los servicios en la nube. Por ejemplo, para supervisar y detectar si el servicio en la nube se está utilizando como plataforma para atacar a otros o si se están filtrando datos sensibles desde el servicio en la nube. Los controles de acceso apropiados deben asegurar el uso de las capacidades de monitorización. Las capacidades deben proporcionar acceso sólo a la información sobre las instancias del servicio en la nube del cliente. El proveedor debe proporcionar documentación de las capacidades de supervisión del servicio al cliente. La monitorización debe proporcionar datos consistentes con los registros de eventos descritos en la cláusula 12.4.1 ISO 27002:2013 y ayudar con términos de SLA.

ID	**SEG-13**
Nº control	27002-12.1.2
Nombre	Gestión de cambios
Descripción	Se han de controlar los cambios en el sistema que pudieran afectar a la seguridad.
Requisitos	El proveedor debería proporcionar al cliente la información sobre los cambios que potencialmente pudieran afectar al servicio. En concreto, se ha de proporcionar la siguiente información sobre los cambios: - Categoría del cambio; - Fecha y hora del cambio; - Impacto; - Funcionalidad afectada; - Tiempo real de interrupción del servicio; - Descripción técnica del cambio en el servicio en la nube o en los sistemas base en los que está basado y el procedimiento detallado del Plan de Marcha Atrás si fuera necesario; - Notificación del inicio y fin del cambio.

ID	**SEG-14**
Nº control	27002-12.1.3
Nombre	Gestión de la capacidad

Descripción	Se ha de monitorizar el uso de los recursos, así como realizar estimaciones de las necesidades de incremento de la capacidad para asegurar que se cumplen los objetivos de rendimiento que han sido contratados.
Requisitos	El proveedor ha de poner a disposición del cliente la información que le permita comprobar que la capacidad del servicio (ej. espacio en disco, rendimiento, número de usuarios concurrentes, etc.) es adecuada a las necesidades del cliente, así como para anticipar un posible crecimiento en el número de usuarios o en las funcionalidades ofrecidas. La oferta debe proporcionar información sobre los límites teóricos de proceso de la solución propuesta en cuanto a usuarios y accesos concurrentes así como proponer planes de escalabilidad de la arquitectura para diferentes tramos de crecimiento.

ID	**SEG-15**
Nº control	27002-12.1.4
Nombre	Separación de entornos de desarrollo, pruebas y producción.
Descripción	Los entornos de desarrollo, pruebas y producción deberán estar separados para reducir los riesgos de accesos no autorizados o cambios en los entornos de producción.
Requisitos	La solución debe contemplar al menos los siguientes entornos de ejecución: - Entorno de pruebas/desarrollo, para proporcionar un escenario de validación de configuraciones e integraciones con los diferentes servicios. - Entorno de producción.

ID	**SEG-16**
Nº control	27002-12.2.1
Nombre	Controles contra el código malicioso
Descripción	Se han de implementar controles de detección, prevención y recuperación para proteger contra el código malicioso (malware).
Requisitos	El proveedor del sistema ha de implementar controles que permitan la detección de código malicioso (malware) y evite su ejecución.

ID	**SEG-17**
Nº control	27002-12.3.1

Nombre	Copias de seguridad
Descripción	Se han de realizar y probar periódicamente copias de seguridad.
Requisitos	Se habrá de realizar copia de seguridad de todos los componentes tecnológicos del sistema. Aquellos componentes de la solución tecnológica implementada que pudieran encontrarse alojados en el cliente habrán de poder ser integrados con los procedimientos y tecnología de backup ya existentes. El proveedor debe garantizar que las copias de seguridad son funcionales. Se deberá garantizar que las copias de ficheros con información de carácter personal, si existieran, no se conservaran por más tiempo que el periodo de retención permitido en virtud de la ley de protección de datos (artículo 4.5 de la Ley 15/1999)

ID	**SEG-18**
Nº control	27002-12.4.1
Nombre	Registro de eventos
Descripción	Se ha de almacenar y revisar de forma regular un registro de eventos de las actividades de los usuarios, errores y otros eventos de seguridad. Estos registros deberán mantenerse por un tiempo de 5 años.
Requisitos	El sistema de gestión del patrimonio ha de almacenar eventos de los accesos satisfactorios y fallidos de los usuarios, las actividades realizadas por estos en el sistema en el uso de las funcionalidades de negocio. Así mismo se deberán almacenar eventos de los accesos satisfactorios y fallidos de los usuarios privilegiados y sus acciones relacionadas tanto con la gestión de usuarios (ej. altas y bajas de usuario) como con la asignación de los derechos de acceso. Esta información ha de poder ser revisada de forma sencilla (por ejemplo, mediante la generación de informes) por parte de los administradores del cliente.

ID	**SEG-19**
Nº control	27002-12.4.2
Nombre	Protección de Registro de eventos
Descripción	Los registros de eventos deben estar protegidos contra la manipulación y el acceso no autorizado.

Requisitos	Se debe proteger el acceso contra cambios no autorizados a la información del registro. Los archivos de registro no deben ser editados o eliminados, ya que si los datos pueden ser modificados o borrados, su existencia puede dar una falsa sensación de seguridad.

ID	**SEG-20**
Nº control	27002-12.4.3
Nombre	Registro de actividad del operador y administrador del sistema
Descripción	Las actividades de los operadores y administradores del proveedor se han de almacenar en un registro protegido y se han de revisar de forma regular.
Requisitos	El proveedor ha de registrar las actividades realizadas por parte de los operadores y administradores del sistema en relación con la información asociada al sistema de gestión del patrimonio del cliente, y dicha información habrá de estar disponible ante una posible solicitud por parte del cliente.

ID	**SEG-21**
Nº control	27002-12.6.1
Nombre	Gestión de vulnerabilidades técnicas
Descripción	Se ha de obtener periódicamente información sobre las vulnerabilidades existentes en las tecnologías utilizadas para la provisión del servicio en la nube, evaluar la exposición del sistema a dichas vulnerabilidades, y tomar las medidas oportunas para atajar los posibles riesgos.
Requisitos	El proveedor ha de proporcionar al cliente la información sobre el procedimiento de gestión de vulnerabilidades e instalación de parches en el sistema a contratar.

ID	**SEG-22**
Nº control	27002-16.1.3
Nombre	Notificación de puntos débiles en la seguridad
Descripción	Todo aquel que utiliza el sistema de información y los servicios debe observar y reportar cualquier deficiencia de seguridad detectada o sospechosa de serlo.
Requisitos	Todo aquel que utiliza el sistema debe informar de estas cuestiones al punto de contacto determinado tan pronto como sea posible a fin de evitar incidentes de

	seguridad. El mecanismo de información debe ser lo más fácil, accesible y disponible como sea posible.

ID	**SEG-23**
Nº control	27002-16.1.4
Nombre	Evaluación y decisión sobre los eventos de seguridad
Descripción	Los eventos de seguridad de la información deben ser evaluados y se debe decidir si han de ser clasificados como incidentes de seguridad.
Requisitos	Se han de analizar los eventos de seguridad y, utilizando una escala de clasificación de incidentes de seguridad, decidir si el evento debe ser clasificado como un incidente y gestionarlo convenientemente.

2.6 Seguridad de las comunicaciones

ID	**SEG-24**
Nº control	27002-13.1.1
Nombre	Controles de red
Descripción	Se han de gestionar y controlar las redes para proteger la información en los sistemas y las aplicaciones.
Requisitos	El proveedor ha de implementar controles de seguridad de red efectivos para asegurar un nivel de protección adecuado al sistema de gestión del patrimonio cuando es accedida desde redes públicas. También deberá asegurar las comunicaciones utilizadas por el proveedor para acceder al sistema.

ID	**SEG-25**
Nº control	27002-13.1.3/27017-9.5.1
Nombre	Segregación de redes y segregación en entornos de virtualización
Descripción	Se debe establecer segregación en redes diferentes de los diversos grupos de sistemas de información, servicios ofrecidos y usuarios del sistema. El entorno virtual del cliente que se ejecuta en un servicio en la nube debe estar protegido de otros clientes y personas no autorizadas.

Requisitos	El proveedor ha de asegurar la segregación en redes diferentes de los sistemas de información que componen el sistema en la nube. Dicha segregación ha de realizarse en base a: - Los distintos clientes del sistema. - Los accesos por parte de los usuarios del sistema y los accesos de los operadores y administradores del proveedor. El proveedor debe aplicar la segregación lógica apropiada de los datos de los clientes, las aplicaciones virtualizadas, los sistemas operativos, el almacenamiento y la red para: - La separación de los recursos utilizados por los clientes en entornos con múltiples clientes. - la separación de la administración interna del proveedor de los recursos utilizados por los clientes. Cuando el servicio en la nube implica arrendamiento múltiple, el proveedor debe implementar controles de seguridad de la información para asegurar el aislamiento apropiado de los recursos utilizados por los diferentes clientes. El proveedor debe considerar los riesgos asociados con la ejecución de software suministrado por otro proveedor asegurando que cumplen todos los requisitos especificados para el servicio.

2.7 Adquisición, desarrollo y mantenimiento de los sistemas de información

ID	**SEG-26**
Nº control	27002-14.2.5
Nombre	Principios de ingeniería segura de sistemas
Descripción	Los principios de ingeniería segura de sistemas se deben establecer, documentar, mantener y aplicar a cualquier sistema de información
Requisitos	La arquitectura propuesta para la solución a implementar en el cliente deberá estar validada y soportada por el fabricante, para asegurar su mantenimiento futuro. El sistema deberá estar configurada de acuerdo con las buenas prácticas recomendadas por el fabricante.

2.8 Gestión de incidentes de seguridad

ID	**SEG-27**
Nº control	27002-16.1.1
Nombre	Responsabilidades y procedimientos

Descripción	Se han de establecer responsabilidades de gestión y procedimientos que aseguren una respuesta rápida, efectiva y ordenada de los incidentes relacionados con la seguridad.
Requisitos	Como parte de las especificaciones del servicio, el proveedor deberá definir los procedimientos y la asignación de responsabilidades entre el cliente y el proveedor para gestionar los incidentes de seguridad. Se ha de proporcionar documentación que incluya al menos la siguiente información: - Ámbito de los incidentes de seguridad que el proveedor notificará al cliente. - Tiempo objetivo de notificación de los incidentes de seguridad desde su detección. - Procedimiento a seguir para la notificación de los incidentes de seguridad. - Información de contacto en relación con la gestión de incidentes de seguridad. - Compromiso de datos personales.

ID	**SEG-28**
Nº control	27002-16.1.5
Nombre	Respuesta a incidentes de seguridad
Descripción	Los incidentes de seguridad deben ser atendidos de acuerdo a los procedimientos documentados.
Requisitos	Los incidentes de seguridad deben recibir un tratamiento desde un punto definido de contacto y de personas relevantes de la organización o partes externas. La respuesta debe contemplar: - La recogida de pruebas tan pronto como sea posible. - La realización de análisis forense de la información de seguridad, según sea necesario. - La progresividad, según sea necesario. - Garantizar que todas las actividades de respuesta involucradas se registran adecuadamente para su análisis posterior. - Que se comunica la existencia del incidente de seguridad o cualquier detalle pertinente del mismo a otras personas internas y externas u organizaciones que tengan necesidad de conocerlas. - Una vez que el incidente ha sido tratado con éxito, se cerrará y grabará formalmente. El análisis post-incidente debe tener lugar, según sea necesario, para identificar el origen del incidente

ID	**SEG-29**
Nº control	27002-16.1.2

Nombre	Notificación de eventos de seguridad
Descripción	Los eventos relacionados con la seguridad se han de reportar lo más rápido posible siguiendo los canales de gestión apropiados.
Requisitos	El proveedor deberá ofrecer mecanismos para que: - El cliente pueda informar al proveedor sobre eventos de seguridad que ha detectado. - El proveedor pueda informar al cliente sobre eventos de seguridad que ha detectado. - El cliente pueda realizar un seguimiento de la situación de un evento de seguridad que ha sido informado.

2.9 Aspectos de seguridad en la gestión de la continuidad del negocio

ID	**SEG-30**
Nº control	27002-17.1.1
Nombre	Planificación de la continuidad de la seguridad
Descripción	La organización deberá determinar sus requisitos de seguridad y continuidad de la gestión de la seguridad en situaciones adversas, por ejemplo durante una crisis o un desastre.
Requisitos	El proveedor ha de asegurar que, en caso de una situación de crisis o un desastre, los requisitos de seguridad se mantienen como parte del plan de continuidad del negocio y del proceso de recuperación ante desastres.

2.10 Cumplimiento normativo

ID	**SEG-31**
Nº control	27002-18.1.1
Nombre	Identificación de la legislación aplicable
Descripción	Se ha de identificar, documentar y mantener actualizada la información relacionada con la legislación relevante que es de aplicación al servicio, así como la forma en la que la organización plantea el cumplimiento de los requisitos normativos.
Requisitos	El proveedor ha de informar al cliente sobre las jurisdicciones legales aplicables a la provisión del servicio. El proveedor habrá de asegurar que la infraestructura técnica en la que almacene la información relativa al sistema de gestión del patrimonio del cliente se encuentra ubicada en territorio de la Unión Europea.

	El proveedor habrá de asegurar el cumplimiento de los requisitos legales que afecten al sistema por su propia naturaleza funcional o por su ubicación geográfica, por ejemplo, en relación con la protección de la información de carácter personal almacenada en el sistema. Si el cliente lo demanda, el proveedor habrá de proporcionar evidencias del cumplimiento de la legislación aplicable y requisitos contractuales.

ID	**SEG-32**
Nº control	27002-18.1.4
Nombre	Protección de datos y privacidad de la información personal
Descripción	Se ha de asegurar la protección de la información relacionada con datos personales que se almacene en el sistema.
Requisitos	El proveedor deberá asegurar el cumplimiento de la legislación en materia de protección de datos personales que sea de aplicación al cliente, como propietario de la información, teniendo la consideración de encargado del tratamiento En concreto, el proveedor deberá dar cumplimiento a los requisitos descritos en el apartado 2.11.

ID	**SEG-33**
Nº control	27002-18.2.1
Nombre	Revisión independiente de la seguridad
Descripción	El enfoque de la organización para gestionar la seguridad así como su implementación (ej. políticas, procesos y procedimientos de seguridad) se ha de revisar de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
Requisitos	El proveedor deberá proporcionar evidencias documentadas e independientes (por ejemplo, mediante un informe de auditoría independiente) de que los procedimientos y controles de seguridad del sistema están siendo aplicados convenientemente. En caso de detectarse algún incumplimiento, se deberán tomar las oportunas acciones correctivas, así como realizar un seguimiento de las recomendaciones abiertas, informando al cliente convenientemente. Adicionalmente, el cliente se reservará el derecho de encargar una auditoría de seguridad del servicio contratado.

2.11 Requisitos adicionales para la protección de datos personales

ID	**SEG-34**
Nº control	27018-A.1.1
Nombre	Cumplimiento de los derechos ARCO
Descripción	Se debe posibilitar el ejercicio de los derechos ARCO.
Requisitos	El proveedor deberá proporcionar la información necesaria para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, e implementar los procesos para que estos derechos puedan ser proporcionados en los plazos legales.

ID	**SEG-35**
Nº control	27018-A.2.1
Nombre	Finalidad de los datos
Descripción	Los datos no podrán utilizarse para otra finalidad diferente para la que fueron recogidos.
Requisitos	El proveedor deberá cumplir con los principios de limitación de la finalidad comprometiéndose a no utilizar los datos para una finalidad diferente a la señalada por el cliente.

ID	**SEG-36**
Nº control	27018-A.5.2
Nombre	Revelación de los datos
Descripción	Toda revelación de los datos deberá ser registrada incluyendo el destinatario y la fecha.
Requisitos	El proveedor deberá registrar la salida de información a terceras partes ya sea en operaciones habituales o por causas legales. Esta información deberá incluir los datos cedidos, la fecha y el destinatario de la información.

ID	**SEG-37**
Nº control	27018-A.7.1
Nombre	Subcontratación del tratamiento

Descripción	La subcontratación del tratamiento de datos personales tendrá que ser aprobada por parte de cliente.
Requisitos	La subcontratación del tratamiento tendrá que ser especificada en el contrato o, en el caso de llevarse a cabo posteriormente, deberá de ser comunicada y aprobada por el cliente con antelación.

ID	**SEG-38**
Nº control	27018-A.9.1
Nombre	Notificación del acceso no autorizado a datos personales.
Descripción	Todo acceso no autorizado a datos personales deberá ser notificado al cliente comunicando si como resultado de este acceso se ha producido perdida, divulgación o alteración de los mismos.
Requisitos	El proveedor debe contemplar la notificación al cliente de accesos no autorizados a datos personales, su pérdida, divulgación o alteración, determinando el tiempo máximo para esta comunicación. La notificación deberá incluir la descripción de los datos comprometidos.

ID	**SEG-39**
Nº control	27018-A.9.2
Nombre	Conservación de políticas de seguridad
Descripción	Disponibilidad de copia de las políticas de seguridad y de los procedimientos de operación.
Requisitos	El proveedor deberá guardar copia de sus políticas de seguridad y procedimientos de operación que hayan sido actualizadas al menos durante un periodo de cinco años.

ID	**SEG-40**
Nº control	27018-A.10.3
Nombre	Constancia de recuperación de datos
Descripción	Control de las operaciones de recuperación de datos.
Requisitos	El proveedor deberá guardar un registro de las operaciones de recuperación que se lleven a cabo: indicando la persona que ejecutó el proceso, los datos

restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso.

3 Prescripciones técnicas

En este apartado se incluyen las especificaciones técnicas para algunos de los controles de seguridad que se habrán de implementar en sistema de gestión del patrimonio histórico-artístico.

3.1 Seguridad de red

ID	**SEG-41**
Descripción	Cortafuegos de aplicación
Requisitos	Se implementarán controles de seguridad a nivel de aplicación para asegurar que la información intercambiada con las distintas interfaces del sistema de gestión del patrimonio está convenientemente protegida. En concreto, se implementará: - Un Web Application Firewall en las interfaces web del sistema. - Proceso de validación de XML (XML Firewall) en las interfaces Web Services del sistema.

3.2 Gestión de identidades y control de acceso

ID	**SEG-42**
Descripción	Autenticación en aplicaciones web (U2A)
Requisitos	Todas las aplicaciones web del servicio en la nube deben proporcionar o poder integrarse con las siguientes funcionalidades de seguridad: - Mecanismos de autenticación fuerte basada en certificados electrónicos. - Soporte de protocolos de federación de identidades basados en estándares como ws-federation, SAML y Oauth

ID	**SEG-43**
Descripción	Uso de certificados electrónicos
Requisitos	Los certificados electrónicos utilizados para los procesos de autenticación y firma por parte de los usuarios del sistema deberán figurar en las listas de confianza de prestadores de servicios electrónicos de confianza emitidas por el Ministerio de Industria, Energía y Turismo de conformidad con el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014. En los procesos que utilicen certificados electrónicos será requerida la comprobación del estado de revocación de los certificados, utilizando para ello los servicios de validación proporcionados por el prestador de servicios electrónicos

	de confianza, preferiblemente en base al protocolo OCSP, si bien el uso de listas de revocación de certificados también será admitido.

ID	**SEG-44**
Descripción	Autenticación en servicios web (A2A)
Requisitos	Todos los servicios web en la nube deben proporcionar o poder integrarse con las siguientes funcionalidades de seguridad: - Proporcionar sistemas de autenticación mediante el estándar WS-Security.

3.3 Seguridad a nivel de aplicación y datos

ID	**SEG-45**
Descripción	Protección de la información intercambiada entre aplicaciones
Requisitos	La información intercambiada con las aplicaciones del cliente habrá de estar protegida incorporando procesos de autenticación, firma electrónica y cifrado como WS-Security, XMLSignature, XMLEncryption y CMS/PKCS7.

4 Conformidad con el Esquema Nacional de Seguridad

ID	**SEG-46**
Descripción	Conformidad con el Esquema Nacional de Seguridad
Requisitos	De conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y el Real Decreto 951/2015, de 23 de octubre, de modificación del 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, el proveedor del sistema de gestión del patrimonio deberá presentar una Declaración de Conformidad con el Esquema Nacional de Seguridad, en base a los criterios y procedimientos previstos en la Guía CCN-STIC-809 «Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento» y Según art. 34 y Anexo III del RD 3/2010, Esta declaración se realizará al menos cada dos años y también en el caso de producirse modificaciones sustanciales en el sistema de información que pudieran repercutir en las medidas de seguridad requeridas.