PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SUMINISTRO DE SUSCRIPCIÓN DE SERVICIOS DE COPIA DE SEGURIDAD Y RESPALDO EN LA NUBE (SaaS) DEL ENTORNO DE OFFICE 365

CONTRATO Nº 224/2022

Área de Planificación y Control

ÍNDICE

1. INTRODUCCIÓN

El objeto de este Pliego es establecer las condiciones que han de regir el suministro como servicio SaaS de copias de seguridad de los datos de Office 365 (M365 en adelante), existente en el correo y en las herramientas colaborativas, de Canal de Isabel II S.A., M.P. (en adelante Canal).

Esta solución debe incluir todas las gestiones necesarias que aseguren la protección y retención a largo plazo de los datos de M365, frente a borrados accidentales, confusión o errores con las políticas de retención, amenazas internas y externas y requisitos legales o de cumplimiento normativo y pueda ser operada por el personal técnico de Canal.

En este pliego se describen los requerimientos técnicos exigidos, especificando una relación de funciones y servicios de la solución y el modelo de gestión.

2. ANTECEDENTES

Canal dispone en la actualidad de una suscripción de M365 en pago por uso que proporciona correo y herramientas colaborativas a los empleados.

Microsoft, fabricante de este producto, se encarga de la disponibilidad de la infraestructura, pero los datos son responsabilidad de Canal, es decir, Microsoft no ofrece de forma nativa ninguna herramienta de copia de seguridad y restauración, solo ofrece un sistema de retención y recuperación de la información basada en papeleras de reciclaje con auto limpieza periódica.

El uso de las aplicaciones de M365 se ha incrementado en Canal y la generación de datos está creciendo de manera significativa. Actualmente, Canal, al no disponer de la solución objeto de este pliego, tiene activada la opción de Litigation Hold como mecanismo provisional de retención de todos los datos y como consecuencia al no poder borrar los datos definitivamente debido a los sistemas de retención, en algunos casos se está llegando al límite del almacenamiento permitido, especialmente en el correo.

Actualmente (27/01/2022) la suscripción de M365 tiene las siguientes volumetrías, que pudieran variar levemente a la fecha de formalización del contrato:

-Usuarios Totales: 4597
-Usuarios con licencia:3160
-Usuarios de Teams: 4597 (4084 internos, 513 invitados)
-Grupos Microsoft 365: 598 (de los cuales: Grupos sin Teams: 105 y Grupos con Teams: 493)
-Espacio Total buzones Exchange en Tb: 30,7 TB
-Espacio Total Onedrive en Tb: 55,5 TB
-Espacio Total Sharepoint en Tb:(Sitios: Clásicos/Grupos/Teams/Personales): 10,3 TB
-Total Sitios: 1891
-Políticas de retención: Ilimitada.

Los servicios de M365 que tienen datos y por tanto requieren la salvaguardia de estos son: Exchange Online, SharePoint Online, Planner, Stream, Videos, OneDrive for Business y Teams.

3. OBJETIVO DEL CONTRATO

El objetivo de este procedimiento es la contratación del "SUMINISTRO DE SUSCRIPCIÓN DE SERVICIOS DE COPIA DE SEGURIDAD Y RESPALDO EN LA NUBE (SaaS) DEL ENTORNO DE OFFICE 365" durante un periodo inicial de 4 años, que permita asegurar el respaldo de los datos y la continuidad del negocio mediante la copia y restauración de los mismos almacenados en los distintos entornos de M365, según las especificaciones técnicas contenidas en el siguiente pliego de prescripciones técnicas.

Canal desea establecer y definir la realización de copias se seguridad de M365 en una solución SaaS mediante un modelo SaaS gestionado por Canal y con soporte del adjudicatario.

Para el cumplimiento de estos objetivos el Adjudicatario debe ofrecer los siguientes servicios:

- Implantación del producto.
- Formación del producto
- Soporte y mantenimiento del producto.

Para poder disponer de una solución y servicios satisfactorios, se han identificado los siguientes factores críticos de éxito:

- Obtener una adecuada adquisición del conocimiento durante la implantación del servicio.
- Realizar una adecuada gestión del conocimiento del sistema, minimizando el tiempo de implantación y asegurando la correcta gestión del conocimiento dentro del equipo (estabilidad y formación).
- Definir un modelo de relación y gestión adecuado para hacer frente a un servicio de soporte.
- Definir los procedimientos de trabajo adecuados con el equipo de Atención al usuario de Canal.

4. REQUISITOS Y SERVICIOS REQUERIDOS

- **Objetos de Productos de M365 sobre los que debe aplicar la copia y restauración**

Exchange Online

- Buzones.
- Grupos (listas de distribución, Microsoft 365)
- Recursos (Salas y equipamiento)
- Contactos
- Buzones compartidos
- Carpetas públicas
- Correos
- Calendarios
- Tareas
- Notas
- Archivado

SharePoint Online

- Ficheros y sus versiones
- Carpetas
- Bibliotecas
- Sitios y subsitios
- Listas y objetos de las listas
- Páginas
- Permisos
- Formularios
- Plantillas

OneDrive

- Ficheros y sus versiones
- Carpetas
- Usuarios y grupos
- Permisos

Teams

- Equipos
- Canales
- Permisos
- Conversaciones
- Metadatos
- Archivos

Planner

- Planes
- Equipos
- Tareas
- Permisos y asignaciones

Stream / Videos

- Ficheros
- Gupos
- Canales
- Permisos

- **Copia de seguridad**

  - La solución debe proporcionar esquemas de copia de seguridad, programación y mecanismos de retención flexibles y personalizables por el usuario.
  - Debe permitir crear diferentes políticas de copia de seguridad para diferentes grupos, con diferentes opciones y horarios.
  - La solución debe permitir seleccionar objetos granulares para la copia de seguridad.
  - Disponer de funcionalidades que permitan la comparación de datos de copia de seguridad con los datos existentes en producción.
  - Entorno Cloud, modalidad Saas con almacenamiento de las copias

- **Frecuencia y tipo de copia**

  - Full Backup inicial.
  - Backup Incremental diario, con flexibilidad horaria programable. Si usa algún tipo de log de transacciones la copia será continua, no estará sujeta a horarios.
  - A demanda.
  - Autodescubrimiento de elementos nuevos.
  - Flexibilidad en las políticas de backup.
  - Los elementos eliminados deben permanecer en las copias.
  - La retención de las copias deber ser como mínimo de 5 años.

- **Seguridad y protección de datos de las copias**

  - Ubicación de las copias de datos y servidores de la solución dentro de la Unión Europea.
  - Al menos 3 copias en ubicaciones distintas.
  - Informes SOC 1 Tipo II (por CPD).
  - Servicios asociados al mantenimiento de los soportes en la U.E.

- Cifrado en tránsito.
- Cifrado en reposo.
- MFA/OTP para control de acceso al servicio.
- Restricción de acceso al servicio por IP.
- Auditoria de acceso al servicio.
- Auditoria de actividad en el servicio.
- Acuerdo de Protección de Datos (DPA) en la U.E.
- Control de acceso. Las copias de seguridad han de estar sometidas a un control de acceso restringido al personal autorizado.
- Acuerdo de Confidencialidad de los datos.
- Acuerdos de Nivel de Servicio (ANS).
- Garantía de integridad e inmutabilidad de las copias.
- Protección de datos, permitir eliminación de datos personales en las copias.
- Debe permitir mecanismos de Modern Authentication de cara a aumentar la seguridad a la hora de configurar las copias.
- Protección contra ransomware en las copias.
- Análisis de fichero antes de realizar la copia para impedir su copia en caso de infección.

- **Interfaz y accesos del servicio de copia.**

  - Acceso Web seguro con diseño intuitivo y amigable.
  - Lenguaje de scripting preferiblemente Powershell para la automatización de tareas.
  - Roles o permisos específicos distintas tareas dentro del servicio:
    - Administrador.
    - Backup.
    - Restore.
    - Eliminación.
    - Reporting.
    - Seguridad.
    - Consulta.
    - Auditor.

  - Funcionalidades avanzadas de búsqueda y eDiscovery tanto a nivel de organización como buzón de correo.
  - Búsquedas granulares en el contenido de las copias.
    - Por usuario.
    - Por mensaje, carpeta, buzón, adjunto, tamaño.
    - Por asunto, remitente, destinatario.
    - Por rango de fechas.
    - Por cadenas de texto, en asunto, cuerpo, remitente y destinatario.

  - Por nombre de fichero.
- Disponibilidad del acceso al servicio según los ANS establecidos

- **Restauración**

  - Procedimientos de restauración sencillos.
  - Tiempos de restauración adecuados.
  - Permitir restaurar en el sitio original.
  - Permitir restaurar en un lugar diferente al original.
  - Permitir restaurar en un fichero.
  - Restauración granular de todos los objetos que se hace backup.
  - eDiscovery
  - Debe ser capaz de recuperar todos los buzones al mismo tiempo (restauración masiva)
  - Debe ser capaz de recuperar todos los OneDrive de la organización al mismo tiempo (restauración masiva).
  - La solución deberá disponer de funcionalidades de restauración de Teams y Sharepoint (incluyendo sus miembros, permisos y configuraciones), archivos, posts.

- **Soporte incidencias y solicitudes.**

  - Soporte 24x7 del adjudicatario
  - Gestión del escalado con el fabricante de la solución ante incidencias del producto.
  - Gestión del escalado de incidencias entre el fabricante de la solución y Microsoft, cuando la incidencia sea responsabilidad de ambos o esté bien definida.
  - Formación
  - Sesión de configuración inicial y formación administradores.

- **Informes**
  - Informes detallados y ejecutivos de las copias de seguridad.
  - Informes detallados de fallos en la copia de seguridad.
  - Informes de restauraciones realizadas.
  - Informes de Autodiscovery “nuevos elementos incluidos”.
  - Informes de periodicidad diaria, semanal y mensual.
  - Envío de informes a través de mail.
  - Informes en formatos conocidos PDF, csv, html o doc.
  - Informes de auditoría.
  - Informes de accesos.
  - Informes de alertas.

- **Otros**

  Posibilidad de descargar todo el contenido almacenado una vez finalizado la relación contractual.

5. CONDICIONES TÉCNICAS DE EJECUCIÓN

El personal técnico de la empresa licitadora que participe en el proyecto deberá estar debidamente capacitado y poseer la experiencia necesaria para el desempeño de sus funciones.
Los horarios para la realización de las distintas intervenciones técnicas objeto del contrato se establecerán de forma consensuada con el personal de Canal.

En caso de que se tenga que realizar cualquier parada de servicio, ésta se realizará en la ventana consensuada con Canal.

El adjudicatario asumirá el servicio de copia de seguridad durante la vigencia del contrato, responsabilizándose de la gestión de las incidencias relacionadas con este sistema.

Deberá disponer además y durante todo el periodo de vigencia del contrato de los recursos técnicos, humanos y materiales adecuados para la prestación del servicio de modo que se garanticen los tiempos de respuesta y de resolución de incidencias detallados en el apartado ACUERDOS DE NIVEL DE SERVICIO, sin coste adicional para Canal.

El precio del contrato se establecerá en un modelo de licenciamiento por uso, atendiendo al número de usuarios activos, precio mensual por licencia del software de copia. Este precio será fijo durante la totalidad del periodo de contrato y en el mismo deberá estar incluido todo lo que el proveedor estime necesario para la prestación el servicio, incluido el espacio de almacenamiento ilimitado para las copias que será facilitado por el adjudicatario, sin que exista ningún otro concepto posterior facturable asociado a este contrato de servicios.
Los usuarios eliminados, mantendrán las copias de seguridad realizadas, aunque no sean ya usuarios activos, y por ende no se facture por ellos.

Como es lógico, la cantidad de usuarios y el tamaño de las copias de seguridad sufrirán variaciones a lo largo de la duración del contrato. Canal podrá incrementar o disminuir el número de usuarios manteniendo las condiciones establecidas para el precio en el contrato.

La recuperación de una copia de seguridad objeto del contrato, así como cualquier otra petición o incidencia relacionada con el servicio, respetará los tiempos de respuesta y resolución descritos en el apartado ACUERDOS DE NIVEL DE SERVICIO.

La duración del periodo de implantación del servicio deberá ser inferior a 1 mes a contar desde la firma del acta de inicio de los trabajos.

Los licitadores indicarán en sus propuestas de puesta en marcha del servicio, el número de jornadas a las que se comprometen para logar la completa implantación de la solución.

Una vez adjudicado el contrato, se consensuará con Canal el Plan de Implantación, estableciendo las fechas y horarios de cada una de las tareas.

Finalizado el periodo de implantación, el licitador deberá proporcionar toda la documentación acerca de las configuraciones realizadas y demás documentación técnica pertinente.

Cualquier cambio en la configuración del sistema de copia deberá ser notificado con anterioridad a Canal, requiriéndose su aprobación antes del despliegue de dicho cambio.

Todas las nuevas operaciones que requieran la intervención del proveedor serán tramitadas mediante apertura de incidencia o petición de servicio respetando los acuerdos de nivel de servicio establecidos para el contrato.

El adjudicatario deberá especificar aquellos requerimientos técnicos necesarios para implantación del servicio.

6. REQUISITOS DE SEGURIDAD MÍNIMOS DEL SOFTWARE COMO SERVICIO

a) El acceso se produce exclusivamente bajo un protocolo seguro que cifre de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad, integridad y disponibilidad (por ejemplo, uso exclusivo de TLS 1.2 o superior, y utilizando sólo suites de cifrado robustas para evitar vulnerabilidades de tipo BEAST (RC4), Lucky13 (CBC), POODLE (SSL 3.0 y TLS 1.0), CRIME (TLS 1.0 compression), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).

b) Todos los formularios, incluidos los de inicio de sesión, tienen que estar protegidos contra ataques de fuerza bruta (uso de CAPTCHA, disociación de los campos “usuario” y “contraseña” en pasos distintos, pero dependientes y controlados, dentro del proceso de inicio de sesión, etc.) y tienen que controlar completamente los caracteres introducidos por el usuario para evitar ataques de tipo Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI), Remote Code Execution (RCE), Inyección SQL, etc.

c) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A., M.P.

d) Que dicho esquema de BBDD sea accedido única y exclusivamente por el/los usuarios de aplicación que vayan a ser utilizados en la conexión del servicio Cloud a dicho esquema de BBDD.
e) Cifrado robusto de los datos propiedad de Canal de Isabel II, S.A., M.P. en la propia BBDD y modelo (cifrado completo o cifrado del dato).

f) Almacenamiento de todos los datos de autenticación de los usuarios en la BBDD mediante el uso de funciones criptográficas seguras conjuntamente con la obligación de utilizar contraseñas complejas (longitud mínima de 10 caracteres, con obligatoriedad de utilizar caracteres alfanuméricos (mezcla de mayúsculas, minúsculas y números) y no alfanuméricos (por ejemplo, signos de puntuación y ortográficos)), establecer un periodo máximo de vigencia y validez de las contraseñas (recomendado un máximo de 60 días) y de implementar un histórico de contraseñas (con un mínimo de 6). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (Password-Based Key Derivation Functions) para el almacenamiento de las contraseñas consideradas como seguras (por ejemplo, PBKDF2 utilizando al menos un generador de números pseudoaleatorios basado en HMAC-SHA1, 5.000 iteraciones para la parte cliente y 100.000 iteraciones para la parte servidora, versiones modernas de bcrypt con un work factor de al menos 12, versiones modernas no vulnerables de Argon2 (Argon2d), etc.).

g) Exista la posibilidad de uso de:

- Un esquema XML para el intercambio de datos de autenticación y autorización (por ejemplo, SAML 2.0) e implementaciones de seguridad a nivel del mensaje.
- OAuth 2.0 como framework de autorización y OpenID Connect (OIDC) como protocolo de autenticación en las APIs existentes.
- SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.

h) En caso de existir Web Services que puedan ser consumidos desde Canal de Isabel II, S.A.,M.P., deben estar securizados a nivel de mensaje, especificando la forma de firmar y cifrar los mensajes de tipo SOAP, a través de la especificación WS-Security. Por tanto:

- Los servicios deben estar autenticados, preferentemente con WS-Security Tokens
- Los usuarios deben ser autenticados vía SAML 2.0.
- La integridad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Signature.
- El no repudio debe estar garantizado a través del uso de WS-Signature o WS-Adressing.
- La confidencialidad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Encryption.
- Debe hacerse uso de una política de seguridad (WS-Policy).

i) Exista la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, ya sea mediante el uso de certificados electrónicos reconocidos (como, por ejemplo, DNIe), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.

j) Todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) han sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP, WASC) para comprobar que existen y que han sido implementadas correctamente.

k) Se almacenará de forma segura (garantía de acceso, recuperación y no modificación) y se revisará de forma regular el registro de eventos de las actividades de los usuarios (errores y eventos de seguridad). Estos registros deberán mantenerse al menos durante cinco (5) años.

l) El proveedor comunicará inmediatamente a Canal de Isabel II, S.A., M.P. todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas, así como las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades.

m) El proveedor del servicio Cloud, en caso de que haya evidencias demostrables de que un incidente de seguridad en Canal de Isabel II, S.A. es imputable a él, se compromete a elaborar un informe pormenorizado y exhaustivo del incidente en el que hará constar, como mínimo, la siguiente información:

- Descripción del incidente.
- Origen del incidente.
- Descripción cronológica de los hechos del incidente.
- Descripción de las acciones preventivas/correctivas llevadas a cabo por el proveedor del servicio Cloud.
- Evaluación de los recursos humanos pertenecientes al equipo de trabajo asignado a la prestación del servicio Cloud contratado por Canal de Isabel II, S.A., M.P. y que han sido necesarios para el análisis y resolución del incidente.

Dicho informe, una vez finalizado, se remitirá al responsable del proveedor en Canal de Isabel II, S.A. quien a su vez lo remitirá a la Dirección de Seguridad.

Los sistemas de información en los que se sustenten los servicios SaaS prestados por el adjudicatario deberán ser conformes con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) o cumplir con las medidas desarrolladas en las correspondientes guías del CCN-STIC o, en caso contrario, deberán adecuarse a ello en el plazo indicado por la disposición transitoria única del RD 311/2022 de 3 de mayo.

7. ACUERDOS DE NIVEL DE SERVICIO

Para la gestión del cumplimiento de los compromisos del Adjudicatario en la prestación del servicio, el ofertante deberá proponer un Acuerdo de Nivel de Servicios (ANS) que Canal considere suficiente para comprobar la calidad del servicio.

Los ANS definidos por Canal son los siguientes:

Código	Descripción	Tiempo Resolución
INC01	Indisponibilidad o fallo de acceso al servicio con afectación a la realización de copias o restauración.	8 horas
INC02	Indisponibilidad o fallo de acceso al servicio sin afectación a la realización de copias o restauración.	16 horas

INC03	Indisponibilidad o fallo de acceso al servicio afectando a la restauración de elementos.	16 horas
INC04	Fallo o indisponibilidad de acceso a servicio afectando a servicios complementarios (reporting, roles, búsquedas)	24 horas
INC05	Incidentes de Seguridad y vulnerabilidades que puedan comprometer los datos del servicio y la copias	3 horas

8. FORMACIÓN

Se planificará la fase de formación de la herramienta para el personal de administración de Canal.

Se especificarán las sesiones antes, durante y después de la implementación del servicio.

9. ENTEGRABLES

- Documento requerimientos para la implementación de la plataforma y accesos.
- Documento de instalación y configuración.
- Manual de operaciones.
- Plan de pruebas.
- Manual y documentación formativa.

La documentación se entregará en formato Word o PDF.

10. REQUISITOS DE SEGURIDAD

El proveedor de servicios Cloud deberá cumplir uno de los siguientes requisitos:

- disponer de certificación del Esquema Nacional de Seguridad nivel medio en cuyo caso se deberá aportar.

  O

- Garantizar los requisitos que se detallan en el fichero *"224-2022-Requisitos_Seguridad.xlsx"* anexo a este pliego. Para la documentación de estos se utilizará dicho fichero y se podrán añadir además los documentos que se consideren necesarios.

11. ESTRUCTURA DE LAS OFERTAS

Las empresas licitadoras deberán presentar de forma precisa, estructurada, clara y concisa sus propuestas.

La oferta técnica se atendrá al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.

Firmado electronicamente por: Jesus Plaza Rubio
En la fecha y hora 30.01.2023 13:34:51 CET

JEFE DE ÁREA PLANIFICACIÓN, CONTROL Y SEGURIDAD

Firmado electronicamente por: RAFAEL EGIDO BLÁNDEZ
En la fecha y hora 30.01.2023 14:59:56 CET

SUBDIRECTOR SISTEMAS INFORMÁTICOS
Delegación por Ausencia: Rafael Egido Blández

Firmado electronicamente por: JUAN SÁNCHEZ GARCÍA
En la fecha y hora 01.02.2023 14:45:02 CET

DIRECTOR DE INNOVACIÓN E INGENERÍA