DATAPRIUS

Plantilla de Cumplimiento de Medidas de Seguridad ENS e ISO/IEC 27001:2022

Documento base para responder cuestionarios de seguridad de clientes, auditores y departamentos de arquitectura / riesgos

Objetivo de uso

Evitar la cumplimentación manual y repetitiva de plantillas de terceros. Este documento aporta respuestas estándar, una matriz de equivalencia ENS/ISO 27001 y un registro de evidencias para que el cliente o su auditor pueda completar su propio cuestionario a partir de información homogénea y controlada.

Campo	Valor sugerido
Versión	v1.0 - Base inicial
Fecha	19/05/2026
Propietario	Dataprius / Responsable de Seguridad
Clasificación	Confidencial - entregar bajo NDA. Incluye detalles técnicos no públicos
Ámbito	Servicio SaaS Dataprius para almacenamiento, gestión documental e intercambio seguro de ficheros
Normas de referencia	ENS (RD 311/2022), ISO/IEC 27001:2022, RGPD/LOPDGDD, buenas prácticas OWASP/CIS cuando apliquen

1. Criterio de uso ante cuestionarios de clientes

- ✓ Entregar este documento como "**Declaración de Cumplimiento y Medidas de Seguridad del Servicio**" junto con el contrato de encargado de tratamiento RGPD y la documentación pública/privada de evidencias.
- ✓ **No rellenar plantillas extensas de terceros salvo que exista alcance definido, NDA firmado y aceptación de coste profesional cuando requiera análisis individualizado, reuniones técnicas o respuestas no estándar.**
- ✓ Distinguir entre los controles propios de Dataprius y controles heredados del proveedor cloud, controles a configurar por el cliente y cuestiones no aplicables al servicio SaaS.
- ✓ No se entregan detalles sensibles como rangos IP internos, diagramas detallados, configuraciones de firewall, inventarios completos o informes de pentesting completos sin NDA y sin limitar destinatarios.
- ✓ Cuando el cliente integra Dataprius con otros sistemas, solicitar la descripción de esa integración, flujos, credenciales, API, tercero interviniente y controles de la otra parte. La seguridad de la integración no depende solo de Dataprius, y Dataprius no entrega más documentación, salvo que se le facilite integra toda esta información.

Dataprius facilita una documentación base de cumplimiento, medidas técnicas y organizativas, localización de infraestructuras, régimen RGPD, trazabilidad y seguridad del servicio. Los cuestionarios específicos de cada entidad deberán ser completados por el cliente o su auditor a partir de esta documentación, salvo contratación expresa de servicios profesionales de soporte a auditoría.

2. Alcance de la plantilla

Incluido	Fuera de alcance / requiere análisis adicional
Servicio SaaS Dataprius, arquitectura funcional, medidas generales de seguridad, datos tratados, repositorios, backup, continuidad, trazabilidad, RGPD y correspondencia ENS/ISO 27001.	Integraciones específicas del cliente, configuración de identidades federadas del cliente, redes internas del cliente, aplicativos de terceros integrados, tratamiento de datos de tarjeta, documentación clasificada o requisitos regulatorios propios no comunicados.
Respuestas reutilizables a aptdo. tipo P(S)A: mapa de solución, seguridad, riesgos y datos.	Rellenar formularios propietarios que exigen decisiones de arquitectura interna del cliente o validación por sus áreas de riesgos, arquitectura, seguridad, DORA/outsourcing o FinOps.
Evidencias públicas y evidencias privadas bajo NDA.	Informes completos de auditoría, pentest o vulnerabilidades sin anonimizar, salvo procedimiento controlado.

2. Ficha resumen de la solución Dataprius

3.

Apartado	Respuesta estándar
Descripción	Dataprius es un servicio SaaS de archivos en la nube para empresas, orientado a almacenamiento, organización, edición, intercambio y trazabilidad de documentos sin depender de sincronización masiva en los equipos de usuario.
Tipo de solución	Producto de tercero / SaaS operado por Dataprius. El cliente consume el servicio mediante aplicación de escritorio, acceso web, aplicaciones móviles y, cuando aplique, integraciones API o aplicaciones web integradas.
Modelo de responsabilidad	Dataprius opera la plataforma SaaS y sus medidas de seguridad. El cliente conserva la responsabilidad sobre alta/baja de usuarios, permisos asignados, clasificación de la información, usos autorizados e integraciones con terceros.
Datos tratados	Ficheros y metadatos asociados al uso del servicio: usuarios, permisos, carpetas, acciones, trazabilidad, incidencias y datos necesarios para la prestación del servicio y cumplimiento contractual/RGPD.
Infraestructura	Servicio alojado sobre cloud soberanía europea de Microsoft Azure Europa como infraestructura de almacenamiento y computación, con ubicaciones europeas y redundancia geográfica según configuración vigente.
Cifrado	Comunicaciones cifradas y almacenamiento cifrado en reposo. Los ficheros se almacenan por bloques y no como archivo completo tradicional.
No aplicabilidad inicial PCI DSS	Salvo que un cliente utilice el servicio para almacenar, transmitir o procesar datos de tarjeta por decisión propia, Dataprius no realiza procesamientos de pagos/cobros como PAN/CVV/SAD. Estos usos están prohibidos, salvo que esté expresamente contratado con Dataprius.

4. Respuestas base para plantillas

Formato recomendado: copiar el bloque aplicable al apartado de la plantilla del cliente y adjuntar esta plantilla completa como evidencia general.

4.1 Apartado 5.2 - Mapa de la solución

Campo de la Plantilla	Respuesta base para Dataprius
Mapa de la solución	**Solución SaaS multiusuario de gestión de archivos.** Los usuarios autorizados acceden al servicio mediante aplicación de escritorio, navegador web o app móvil. Las operaciones se realizan contra la plataforma Dataprius, que gestiona autenticación, permisos, carpetas, trazabilidad, almacenamiento y recuperación.
Actores y roles	Cliente/empresa contratante; administradores del entorno cliente; usuarios internos; usuarios externos invitados o clientes autorizados; soporte Dataprius; proveedores cloud de infraestructura; integradores autorizados si existe integración API.
Componentes	Aplicaciones cliente, portal web, servicios de aplicación Dataprius, repositorios de metadatos, almacenamiento de ficheros por bloques, registros de actividad/seguridad, backup y monitorización.
Interfaces	Interfaz web, aplicación de escritorio, apps móviles y API/integraciones cuando estén contratadas y documentadas. Las integraciones concretas deberán ser descritas por el cliente/integrador, incluyendo flujos, credenciales, tratamiento de datos y medidas compensatorias.
Flujo de datos	El usuario autenticado solicita acceso a carpetas/ficheros. La plataforma valida identidad y permisos, registra la actividad, cifra la comunicación y gestiona la lectura/escritura sobre almacenamiento cloud. La información puede replicarse localmente mediante descargas o edición temporal controlada por el usuario/cliente.
Modelo origen/futuro	No aplica como evolución interna del cliente salvo integración específica. Dataprius se consume como servicio SaaS estándar; cualquier modificación futura de integración, API o automatización deberá documentarse como cambio de alcance.

4.2 Apartado 5.4 – Seguridad

Requisito	Respuesta estándar	Correspondencia ENS / ISO 27001	Evidencias
Gobierno de seguridad	Dataprius mantiene políticas, procedimientos y responsables internos para la gestión de seguridad, privacidad, continuidad, operación y respuesta a incidentes. Existe un punto de contacto de seguridad para clientes.	**ENS:** marco organizativo y política de seguridad. **ISO 27001:** A.5.1, A.5.2, A.5.31, A.5.36.	**Política de seguridad, organigrama, contrato RGPD, documento de seguridad.**
Cadena de suministro	La prestación se apoya en proveedores cloud y servicios auxiliares declarados. La relación con terceros debe gestionarse mediante evaluación, contratos, garantías de seguridad y revisión periódica.	**ENS:** cadena de suministro, servicios externalizados. **ISO 27001:** A.5.19-A.5.23.	**Lista de proveedores, DPA/subencargados, certificaciones del proveedor cloud.**
Gestión de activos	Existe inventario de activos tecnológicos, software base, componentes, servicios cloud, repositorios y responsables asociados al servicio.	**ENS:** gestión de activos. **ISO 27001:** A.5.9, A.5.10, A.8.9.	**Inventario interno, CMDB, lista controlada de servicios.**
Dispositivos de movilidad	Dataprius no requiere que la información resida permanentemente en portátiles o móviles del cliente. El cliente debe controlar descargas, dispositivos autorizados, bloqueo, cifrado local y MDM cuando corresponda.	**ENS:** Protección de equipos/soportes. **ISO 27001:** A.6.7, A.8.1, A.8.10.	**Manual de configuración cliente, política de uso aceptable.**
Vulnerabilidades	Debe existir un proceso documentado de gestión de vulnerabilidades: identificación, priorización por criticidad, remediación, verificación y registro. Para compromisos de SLA estrictos se recomienda pactar una tabla de plazos por criticidad.	**ENS:** gestión de vulnerabilidades, protección y explotación. **ISO 27001:** A.8.8, A.8.9.	**Procedimiento de vulnerabilidades, registros de remediación, informes ejecutivos.**
Pentest y auditorías	En SaaS, Dataprius puede facilitar bajo NDA informes ejecutivos de auditorías/pentest o certificados equivalentes. El coste del NDA deberá ser abonado por el cliente.	**ENS:** auditoría y revisión. **ISO 27001:** A.5.35, A.8.29, A.8.34.	**Informe ejecutivo de pentest, certificado, plan de acciones.**
Parcheado	El software base y componentes se mantienen actualizados conforme a criticidad, compatibilidad y	**ENS:** mantenimiento y protección frente a vulnerabilidades.	**Política de parches, registros de cambio,**

	procedimiento de cambio. Los parches críticos de seguridad son prioritarios sobre el ciclo ordinario.	**ISO 27001:** A.8.8, A.8.9, A.8.32.	**evidencias de actualización.**
Identidades y accesos	La solución aplica mínimo privilegio, segregación de roles, perfiles de usuario y trazabilidad de accesos. La gestión de altas, bajas y permisos de cada tenant corresponde al administrador designado por el cliente.	**ENS:** control de acceso. **ISO 27001:** A.5.15-A.5.18, A.8.2, A.8.3, A.8.5.	**Manual de roles/permisos, registros de acceso, revisión de permisos.**
Cuentas privilegiadas	Las cuentas administrativas se limitan al personal autorizado, se protegen con controles reforzados y se revisan periódicamente. Se recomienda MFA para accesos administrativos y trazabilidad completa.	**ENS:** privilegiados y administración. **ISO 27001:** A.8.2, A.8.5, A.8.15.	**Relación de roles, procedimiento PAM/MFA, logs.**
Almacenamiento de contraseñas	Las credenciales se almacenan encriptadas. Se utiliza algoritmos de hash robusto con parámetros actualizados. El algoritmo exacto se documenta internamente y solo se comunicará bajo NDA si procede.	**ENS:** autenticación. **ISO 27001:** A.5.17, A.8.5, A.8.24.	**Diseño técnico de autenticación, política de contraseñas.**
Concienciación	El personal con acceso al servicio debe recibir formación y recordatorios en seguridad, privacidad, confidencialidad, gestión de incidentes y tratamiento de datos.	**ENS:** formación y concienciación. **ISO 27001:** A.6.3.	**Plan de formación, registros de asistencia.**
Copias de seguridad	Dataprius mantiene copias de seguridad y redundancia acordes con el servicio. Las copias están protegidas, cifradas cuando aplique y con pruebas periódicas de restauración. Los objetivos RPO/RTO se documentan por nivel de servicio.	**ENS:** continuidad, copias y recuperación. **ISO 27001:** A.5.30, A.8.13.	**Procedimiento backup/restore, resultados de prueba, definición RTO/RPO.**
Malware y ficheros seguros	La plataforma incorpora medidas de protección frente a código dañino y validación de tipos de fichero cuando aplique. El cliente debe mantener controles endpoint y política de tipos de archivo permitidos.	**ENS:** protección frente a código dañino. **ISO 27001:** A.8.7, A.8.12.	**Política de ficheros, evidencias antimalware, configuración.**
Protocolos seguros y cifrado	Todo acceso privado debe realizarse mediante protocolos cifrados y algoritmos robustos. La información en reposo debe estar cifrada según controles aplicables y responsabilidades de Dataprius/proveedor cloud.	**ENS**: cifrado, comunicaciones y protección de información. **ISO 27001:** A.8.20-A.8.24.	**Configuración TLS, documento de seguridad, evidencias cloud.**

Bastionado y obsolescencia	Los sistemas se instalan con configuración segura, servicios mínimos, actualizaciones de seguridad y sin software fuera de soporte.	**ENS:** configuración segura. **ISO 27001:** A.8.9, A.8.20, A.8.21.	**Guías hardening, inventario de versiones, registros de actualización.**
Desarrollo seguro	El ciclo de vida de desarrollo incorpora revisión, pruebas, control de cambios, segregación de entornos, buenas prácticas OWASP y validación previa a producción.	**ENS:** desarrollo seguro y ciclo de vida. **ISO 27001:** A.8.25-A.8.31.	**Procedimiento SDLC, repositorios, evidencias de pruebas.**
Seguridad en red	La plataforma se protege mediante controles perimetrales, reglas de mínimo acceso, segmentación, monitorización y, cuando aplique, WAF/IDS/medidas antiDDoS heredadas o propias.	**ENS:** comunicaciones, segregación y protección perimetral. **ISO 27001:** A.8.20-A.8.22.	**Arquitectura de red de alto nivel, evidencias cloud, configuración WAF/Firewall bajo NDA.**
Seguridad física	Los controles físicos de CPD son responsabilidad del proveedor cloud en la parte de infraestructura. Dataprius conserva las evidencias contractuales/certificaciones del proveedor aplicables.	**ENS:** instalaciones. **ISO 27001:** A.7.1-A.7.14.	**Certificaciones y documentación del proveedor cloud.**
Monitorización	La solución registra eventos de seguridad y operación con trazabilidad suficiente, mantener logs según política de retención y proporcionar alertas/seguimiento 24x7 cuando aplique al servicio.	**ENS:** registro, monitorización y detección. **ISO 27001:** A.8.15, A.8.16.	**Política de logs, registro de seguridad, dashboards, evidencias de alertas.**
Incidentes	Dataprius dispone de procedimiento de gestión de incidentes: detección, clasificación, contención, erradicación, recuperación, comunicación, conservación de evidencias y lecciones aprendidas. Los plazos de notificación contractuales son los especificados en las cláusulas de los T&C.	**ENS:** gestión de incidentes. **ISO 27001:** A.5.24-A.5.28.	**Procedimiento de incidentes, registro, plantilla de comunicación, simulacros.**
PCI DSS	No aplica por defecto si Dataprius no almacena, procesa o transmite datos de tarjeta por diseño. Si el cliente usa el servicio para esos datos, debe abrirse evaluación específica y medidas contractuales.	**ENS/ISO:** cumplimiento legal/contractual. **ISO 27001:** A.5.31, A.5.34.	**Declaración de no tratamiento de PAN/CVV/SAD; cláusula de uso prohibido o evaluación PCI.**

4.3 Apartado 5.5 – Riesgos

Subapartado	Respuesta base
Geolocalización	El proveedor cloud es Azzure con ubicación en Europa de almacenamiento principal y backups (Soberanía de datos europea)
Contractual	Contrato RGPD de encargado de tratamiento (DPA), condiciones de subencargados, SLA, soporte y, si el cliente lo exige, anexo de seguridad o cláusulas DORA/outsourcing cuando proceda y bajo NDA.
Seguridad del desarrollo	Metodología de desarrollo seguro, separación de entornos, revisión de cambios, pruebas y controles SAST/DAST/IAST. Plan de mejora.
Plataforma y actualizaciones	Política de parcheado, ventanas de mantenimiento, priorización de vulnerabilidades y control de versiones.
Gestión de cambios	Todo cambio significativo debe registrarse, aprobarse, probarse y desplegarse con posibilidad de reversión.
Continuidad de negocio	Plan de continuidad, responsables, escenarios, pruebas y resultados.
Continuidad y resiliencia TIC	Declarar criticidad, redundancia, backup, restauración, RTO/RPO, monitorización y procedimiento de recuperación.

4.4 Apartado 5.6 - Datos

Campo	Respuesta base
Modelo de datos	Ficheros aportados por el cliente y metadatos necesarios para la prestación del servicio: usuarios, grupos, permisos, carpetas, actividad, trazabilidad, incidencias, configuración, registros técnicos y facturación/soporte.
Titularidad	Los datos y documentos son titularidad/responsabilidad del cliente. Dataprius actúa como proveedor/encargado del tratamiento en los términos del contrato RGPD aplicable.
Categorías	Pueden existir datos personales, confidenciales o sensibles según el contenido que el cliente almacene. Dataprius no determina el contenido de los documentos; el cliente debe clasificar y limitar qué información sube al servicio.
Repositorios	Repositorios de ficheros por bloques, base de datos/metadatos, registro de actividad, registro de seguridad, backups y sistemas de monitorización.
Cifrado	Comunicaciones cifradas y cifrado en reposo en almacenamiento cloud conforme a la configuración vigente. Las descargas locales quedan bajo responsabilidad del cliente y sus políticas endpoint.
Backups	Copias de seguridad y redundancia conforme al nivel de servicio. Se realizan con periodicidad, retención, ubicación y pruebas de restauración aprobadas internamente.
Transferencias internacionales	La documentación pública de Dataprius enfatiza soberanía europea/no transferencia fuera de la UE para almacenamiento
Supresión/devolución	A la baja del servicio o por instrucción válida, aplicar procedimientos de devolución, exportación o borrado conforme a contrato, RGPD y política de retención.

5. Matriz de equivalencia ENS / ISO 27001 para respuestas a auditorías

La correspondencia es funcional, no es una equivalencia jurídica exhaustiva remitiéndose a la declaración de Aplicabilidad formal con evidencias fechadas.

Dominio de control	ENS - enfoque funcional	ISO/IEC 27001:2022	Uso en cuestionarios
Política, gobierno y responsabilidades	Política de seguridad, responsables diferenciados, procedimientos, comité/POC, revisión de dirección.	**A.5.1, A.5.2, A.5.4, A.5.31, A.5.36**	Aporta marco documental y RACI; las decisiones del cliente se validan por su área de seguridad.
Inventario y gestión de activos	Inventario de activos, servicios, repositorios, software base y propietarios.	**A.5.9, A.5.10, A.8.9**	Mantener inventario interno; entregar resumen no sensible.
Control de accesos e identidades	Mínimo privilegio, gestión de usuarios, autenticación, revisión de derechos, segregación de funciones.	**A.5.15-A.5.18, A.8.2, A.8.3, A.8.5**	Cliente administra sus usuarios y permisos; Dataprius gestiona roles de operación y soporte.
Criptografía y protección de datos	Cifrado en tránsito, cifrado en reposo, gestión de claves, protección de soportes y comunicaciones.	**A.8.20-A.8.24**	Protocolos y cifrado de alto nivel; no divulgar secretos o configuraciones sensibles.
Copias, continuidad y resiliencia	Backups, pruebas de restauración, redundancia, continuidad, RTO/RPO, recuperación ante desastre.	**A.5.29, A.5.30, A.8.13**	RTO/RPO aprobados; resultados ejecutivos de pruebas.
Vulnerabilidades, parches y configuración	Gestión de vulnerabilidades, hardening, parches, configuración segura y control de obsolescencia.	**A.8.8, A.8.9, A.8.32**	Política y resumen de cumplimiento; detalle técnico bajo NDA.
Desarrollo seguro	Ciclo de vida seguro, control de cambios, pruebas, segregación dev/test/prod, OWASP.	**A.8.25-A.8.31**	Aportar SDLC, evidencias de pruebas y gestión de cambios.
Red y perímetro	Firewalls, reglas de mínimo acceso, WAF/IDS si aplica, segmentación, antiDDoS.	**A.8.20-A.8.22**	Arquitectura de alto nivel; configuraciones exactas no se entregan sin NDA.
Monitorización y registros	Logs, trazabilidad, eventos de seguridad, retención, alertas y revisión.	**A.8.15, A.8.16**	Política de logs y ejemplo anonimizado de registro.
Gestión de incidentes	Detección, clasificación, notificación, respuesta, conservación de evidencias y mejora continua.	**A.5.24-A.5.28**	Plazos contractuales según T&C
Cadena de suministro y cloud	Gestión de terceros, subencargados, acuerdos de seguridad, revisión y servicios cloud.	**A.5.19-A.5.23**	Lista vigente de proveedores y ubicaciones, contratos y certificaciones cloud.
Seguridad física	Controles de CPD, acceso físico, ambiente, soporte y borrado de activos.	**A.7.1-A.7.14**	Evidencias heredadas del proveedor cloud y controles propios de oficinas si aplican.
Personas y confidencialidad	Formación, concienciación, NDA, responsabilidades y salida/cambio de empleo.	**A.6.1-A.6.8**	Registros de formación y compromisos de confidencialidad.
Cumplimiento legal y privacidad	RGPD, LOPDGDD, contratos de encargado, subencargados, privacidad y requisitos contractuales.	**A.5.31, A.5.34**	Contrato RGPD, RAT si aplica, DPA, política de privacidad, procedimiento brechas.

6. Registros de evidencias

ID	Evidencia	Nivel de entrega	Actualización	Observación
E-01	Contrato RGPD / encargado de tratamiento	Público/cliente	Vigente	Se adjunta contrato firmado o enlace a condiciones.
E-02	Documento de seguridad / descripción de medidas	Público	Vigente	URL pública, PDF controlado. Remisión email.
E-03	Lista de proveedores, subencargados y ubicaciones	Público/cliente	Vigente	Revisar ante cambios de cloud/subproveedor.
E-04	Política de seguridad de la información	Confidencial	Anual	Resumen externo y versión interna completa.
E-05	Inventario de activos y componentes	Confidencial	Trimestral	Entrega extracto no sensible.
E-06	Política de control de accesos y roles	Confidencial/cliente	Anual	Incluye altas, bajas, revisión y privilegios.
E-07	Procedimiento de vulnerabilidades y parcheado	Confidencial	Anual	Con SLAs internos aprobados.
E-08	Informe ejecutivo de pentest/auditoría	NDA	Anual o según plan	No entregar detalle explotable.
E-09	Procedimiento backup/restore y prueba de restauración	Confidencial/cliente	Anual	Incluye RPO/RTO aprobados.
E-10	Procedimiento de incidentes y brechas	Confidencial/cliente	Anual	Incluye plantilla de notificación y conservación de evidencias.
E-11	Registros de formación y confidencialidad	Confidencial	Anual	No entregar datos personales innecesarios.
E-12	Certificaciones ENS/ISO/SOC del servicio o proveedor cloud	Público/NDA	Según vencimiento	Declarar solo si el alcance cubre el servicio.

FUENTES

Referencia	Fuente
ENS	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191
CCN ENS	Portal ENS - normativa, ITS y guías STIC serie 800. https://ens.ccn.cni.es/es/normativa
ISO/IEC 27001	ISO/IEC 27001:2022 - Information security management systems - Requirements. https://www.iso.org/obp/ui/en/
Dataprius seguridad	https://dataprius.com/dataprius-descripcion-de-seguridad-del-sistema.html
Dataprius RGPD	https://dataprius.com/blog/cumplimiento-rgpd-real-de-servicio-almacenamiento-nube/