PRODAT®
PROTECCION DE DATOS

Certificado de Implantación y Cumplimiento RGPD – 2025 –

PRODAT PRINCIPADO, S.L. con CIF **B74253410**, empresa líder en cumplimiento normativo y mejora continua de las obligaciones establecidas en las normas de protección de datos, garantiza que:

BIG HEALTH DATA CONSULTING, S.L.

con CIF B52529468

Ha implantado en todos los sistemas pertenecientes a la sociedad las obligaciones establecidas en las siguientes normas de aplicación:

- *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.*

BIG HEALTH DATA CONSULTING S.L. tiene implantadas las medidas de seguridad, técnicas y organizativas que se corresponden a cada uno de los tratamientos de datos realizados y dispone de la figura del Delegado de Protección de Datos (DPD) inscrito en la AEPD.

Asimismo, dispone del preceptivo Sistema de Gestión de Protección de Datos, debidamente actualizado, garantizando el deber de secreto y seguridad de los datos de carácter personal. En el Anexo I se detallan las medidas de seguridad implantadas y auditadas que se aplica a las actividades de tratamiento que desarrolla

Y para que así conste se firma la presente en Oviedo, a 11 de noviembre de 2025

Antonio García Fernández
*CEO **PRO**DAT*

CATÁLOGO DE EMPRESAS Y SOLUCIONES DE CIBERSEGURIDAD
EMPRESA REGISTRADA incibe_

ENTIDAD ADSCRITA
Pacto Digital para la Protección de las Personas

Adecuación Web · Servicio de Adecuación LOPD · Formación · Mantenimiento Soporte Jurídico · Plataforma SIGPAC · Política de Privacidad

PRODAT PRINCIPADO S.L.
C/ Torrecerredo, 4 bajo 33012 OVIEDO 985 114 057
e-mail: asturias@prodat.es Web: www.prodat.es

ANEXO I.

1. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS DEFINIDAS Y DOCUMENTADAS

Las funciones de los usuarios finales se recogen en el DOCUMENTO DE MEDIDAS DE SEGURIDAD de la Organización:

1.1. Relación de usuarios y perfiles de usuarios autorizados perfil

1.2. Circular de medidas de seguridad donde se establecen las obligaciones de todos los usuarios en materia de seguridad y confidencialidad

2. DESIGNACIÓN DE LAS PERSONAS CON FUNCIONES DE CONTROL DE SEGURIDAD

Son las personas autorizadas para conceder, modificar o anular el acceso de los usuarios a:

- los sistemas de información (redes informáticas, ordenadores y equipos, servidores, etc.)
- los sistemas de archivo de documentación en soporte papel

Sus funciones también incluyen implantar las medidas de seguridad recogidas en el Documento de medidas de seguridad para aquellos sistemas de información que controlan. Únicamente se concede el acceso a los usuarios en base a los criterios definidos por BIG HEALTH DATA CONSULTING, S.L. en el Documento de medidas de seguridad y previa autorización de la Dirección.

3. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y REGISTRO DE INCIDENCIAS DE SEGURIDAD

BIG HEALTH DATA CONSULTING, S.L. recoge cuantas incidencias de seguridad se produzcan sobre los datos personales que se trata. Este procedimiento establece los mecanismos de actuación por parte de los usuarios de los sistemas de información para la comunicación, gestión y respuesta ante las incidencias de seguridad. La aplicación del procedimiento se establece para todos los usuarios, tanto empleados o colaboradores externos.

Se interpreta el concepto de incidencia en su sentido más amplio, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan. El Administrador de Sistemas gestiona la implantación del procedimiento de gestión de incidencias y realiza el seguimiento de todas las incidencias en materia de seguridad. Todos los usuarios están fehacientemente informados de la obligación de notificar cualquier incidencia producida en materia de seguridad.

4. PROCEDIMIENTO DE GESTIÓN DE SOPORTES INCLUYENDO SU IDENTIFICACIÓN, INVENTARIO, DESHECHO DE SOPORTES CON BORRADO IRREVERSIBLE O DESTRUCCIÓN

Definimos soporte como aquel objeto físico que almacena o contiene datos o documentos u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. Algunos de los soportes más comunes son:

- Ordenadores, servidores, portátiles, unidades NAS y demás equipos informáticos
- Dispositivos de almacenamiento como discos, cintas, discos ópticos, tarjetas de memoria, unidades de memoria USB, discos duros externos …

- Armarios o archivadores donde se almacenan los documentos

Los soportes y documentos que contengan datos personales siempre permiten identificar el tipo de información que contienen, salvo cuando las características físicas del soporte lo imposibiliten. Todo soporte empleado debe ser inventariado. Dicho inventario se ha incorporado en el Documento de Medidas de seguridad como Anexo IV. Inventario de equipos, soportes y dispositivos de archivo. La salida de soportes y documentos que contenga datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los deben ser autorizados por el responsable del tratamiento o encontrarse debidamente autorizada en el Documento de Medidas de Seguridad. En caso de reutilización de un soporte, se procede a eliminar toda la información almacenada en el mismo mediante el uso de una herramienta específica que impida cualquier recuperación posterior de información.

Cuando se deshecha cualquier documento o soporte que contengan datos de carácter personal debe procederse a su destrucción, de manera que se impida la reconstrucción posterior del documento.

5. CONTROL DE ACCESO EN BASE AL CRITERIO DE MÍNIMO PRIVILEGIO

Los usuarios tienen acceso únicamente a aquellos datos que precisen para el desarrollo de sus funciones. Se encuentran establecidos mecanismos para evitar que un usuario pueda acceder a recursos distintos de los autorizados. Existe una relación actualizada de usuarios, perfiles de usuario y accesos autorizados en el Documento de Medidas de Seguridad. Anexo V. Relación de usuarios y perfiles de usuario autorizados.

Los usuarios que van a tener acceso a tratamiento de datos personales reciben desde su incorporación toda la información relativa al compromiso de confidencialidad y las medidas de seguridad que forman parte de sus obligaciones laborales.

El acceso a datos personales por parte de otras personas que no figuren en el Listado se encuentra estrictamente prohibido y únicamente puede producirse mediante petición firmada del interesado y con autorización por escrito de la Dirección. El personal ajeno con acceso a los locales y recursos de la Organización está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Con los prestadores de servicios que tienen acceso a datos personales se firma el correspondiente Contrato de Encargado de tratamiento conforme al art. 28 RGPD con previsiones estrictas respecto de la subcontratación.

6. IDENTIFICACIÓN Y AUTENTICACIÓN INEQUÍVOCA DE LOS USUARIOS

Los procedimientos seguidos para la identificación y autenticación de los usuarios cuando intentan acceder a los sistemas, las redes o las aplicaciones están basados en la combinación de un código de identificación de usuario y una contraseña robusta. A cada usuario le han sido asignados identificadores individuales tanto para el acceso a los sistemas como para el acceso a las aplicaciones.

7. RENOVACIÓN PERIÓDICA DE LAS CREDENCIALES DE ACCESO

Únicamente las personas designadas para ello tienen competencias para autorizar el alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y datos. Todas las contraseñas deben ser modificadas por el usuario, el menos, con la frecuencia establecida. En los entornos en los que sea posible se

automatiza este requerimiento de caducidad. En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia de la Organización.

8. CIFRADO DE CONTRASEÑAS

Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña. Las contraseñas se almacenan cifradas y ninguna persona tendrá acceso a la descodificación de las mismas. En el caso del sistema y la red, las contraseñas se almacenan cifradas por sus propias herramientas de seguridad. En el caso de las aplicaciones, el cifrado de las contraseñas es realizado por el sistema gestor de bases de datos o por un desarrollo ‘’ad hoc’’ de la propia aplicación.

9. COPIAS DE SEGURIDAD

El Administrador de Sistemas se encarga de controlar la correcta aplicación de los procedimientos de forma que se cumplan los siguientes requisitos:

- Todos los soportes utilizados para las copias de seguridad cumplen las normas relativas a identificación de los soportes, inventariado y almacenamiento con las correspondientes medidas de control de acceso que garantizan que únicamente sean utilizadas por el personal encargado de la ejecución de las copias de respaldo.
- Los procedimientos de copia de seguridad cubren la totalidad de tratamientos automatizados de datos personales incluidos en los servidores, bases de datos, soportes móviles y demás dispositivos.
- La periodicidad de la copia es diaria
- Los procedimientos para la recuperación de los datos garantizan su recuperación en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción
- Cuando se realicen pruebas con datos reales es obligatorio realizar previamente copia de todos los datos.
- Se mantienen varios soportes de copias de seguridad

10. EJERCICIO DE DERECHOS DE LOS INTERESADOS

Los ejercicios de derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad del tratamiento se tramitan y responden conforme al Manual de Atención al Ejercicio de Derechos.

***