DIGITELTS

by MADISON

SEGURIDAD DE LA INFORMACIÓN

Los niveles más exigentes de **seguridad jurídica, seguridad de la información e infraestructura cloud,** son las bases de nuestras soluciones digitales.

DIGITEL TS
by MADISON

Índice de Contenido

1 SEGURIDAD DE LA INFORMACIÓN

1.1 Certificaciones de Seguridad de la Información

Digitel TS tiene un compromiso firme con la Seguridad de la Información constatado por el **Certificado de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013** obtenido de manos de BUREAU VERITAS y por el **Certificado en Materia de Protección de Datos** obtenido de manos de PRODAT, organización especializada en servicios de Consultoría, Auditoría y Outsourcing en el ámbito de protección de datos de carácter personal.

Paralelamente, se dispone del **Certificado de Prestadores de Servicio de Confianza** para el **Servicio de expedición de sellos electrónicos cualificados de tiempo** según el **Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014 (eIDAS)** obtenido de manos de AENOR.

Bureau Veritas Certification

Certificación

Concedida a

TELECYL SA

CL ENRIQUE CUBERO, 9 – 47014 – VALLADOLID – ESPAÑA

Bureau Veritas Certification certifica que el Sistema de Gestión ha sido auditado y encontrado conforme con los requisitos de la norma:

NORMA

ISO/IEC 27001:2013

El Sistema de Gestión se aplica a:

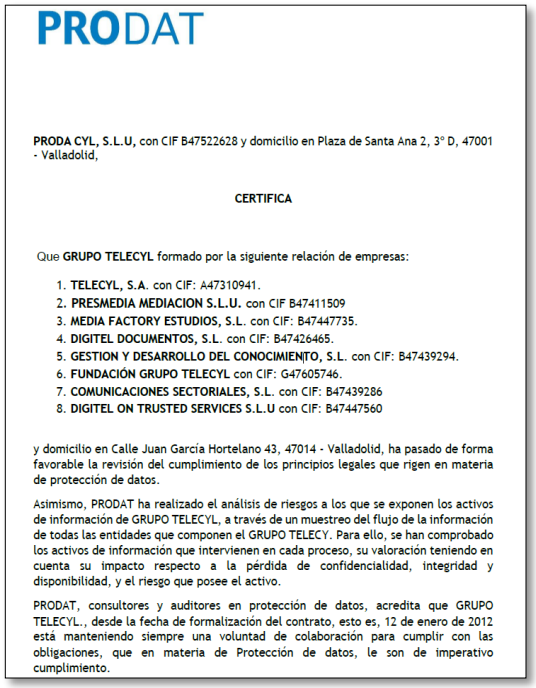
EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE DA SOPORTE A LOS SERVICIOS DE CONSULTORÍA, ACTIVIDADES TECNOLÓGICAS, TRATAMIENTO Y CUSTODIA DE LA INFORMACIÓN DOCUMENTAL ELECTRÓNICA Y GESTIÓN DE ARCHIVOS, EN PROCESOS DE NEGOCIO DE MARKETING. SEGÚN LA DECLARACIÓN DE APLICABILIDAD DEL 17/12/2020.

Número del certificado:	ES117750-1
Aprobación original:	13-02-2018
Certificado en vigor:	13-02-2021
Caducidad del certificado:	12-02-2024

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/Valportillo Primera 22-24, Edificio Caoba, 28108 Alcobendas - Madrid, España
1/1

ENAC CERTIFICACIÓN
Nº 04/C-SG041



PRODAT

PRODA CYL, S.L.U, con CIF B47522628 y domicilio en Plaza de Santa Ana 2, 3° D, 47001 - Valladolid,

CERTIFICA

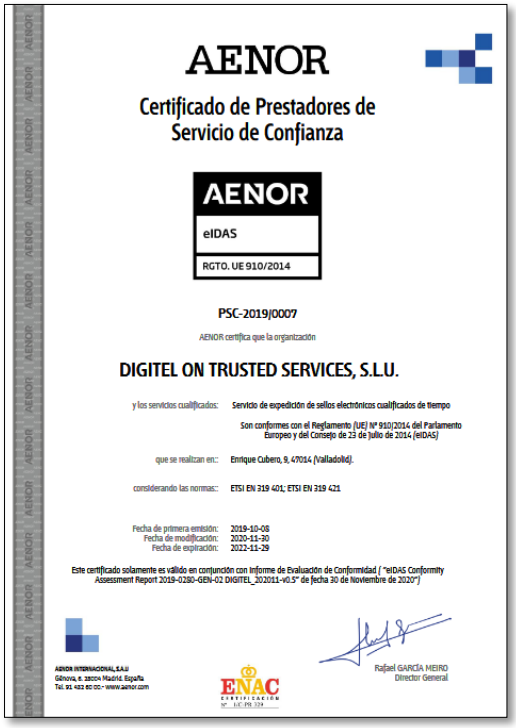
Que **GRUPO TELECYL** formado por la siguiente relación de empresas:

1. **TELECYL, S.A.** con CIF: A47310941.
2. **PRESMEDIA MEDIACION S.L.U.** con CIF B47411509
3. **MEDIA FACTORY ESTUDIOS, S.L.** con CIF: B47447735.
4. **DIGITEL DOCUMENTOS, S.L.** con CIF: B47426465.
5. **GESTION Y DESARROLLO DEL CONOCIMIENTO, S.L.** con CIF: B47439294.
6. **FUNDACIÓN GRUPO TELECYL** con CIF: G47605746.
7. **COMUNICACIONES SECTORIALES, S.L.** con CIF: B47439286
8. **DIGITEL ON TRUSTED SERVICES S.L.U** con CIF: B47447560

y domicilio en Calle Juan García Hortelano 43, 47014 - Valladolid, ha pasado de forma favorable la revisión del cumplimiento de los principios legales que rigen en materia de protección de datos.

Asimismo, PRODAT ha realizado el análisis de riesgos a los que se exponen los activos de información de GRUPO TELECYL, a través de un muestreo del flujo de la información de todas las entidades que componen el GRUPO TELECY. Para ello, se han comprobado los activos de información que intervienen en cada proceso, su valoración teniendo en cuenta su impacto respecto a la pérdida de confidencialidad, integridad y disponibilidad, y el riesgo que posee el activo.

PRODAT, consultores y auditores en protección de datos, acredita que GRUPO TELECYL., desde la fecha de formalización del contrato, esto es, 12 de enero de 2012 está manteniendo siempre una voluntad de colaboración para cumplir con las obligaciones, que en materia de Protección de datos, le son de imperativo cumplimiento.



AENOR

Certificado de Prestadores de Servicio de Confianza

AENOR

eIDAS

RGTO. UE 910/2014

PSC-2019/0007

AENOR certifica que la organización

DIGITEL ON TRUSTED SERVICES, S.L.U.

y los servicios cualificados: Servicio de expedición de sellos electrónicos cualificados de tiempo

Son conformes con el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014 (eIDAS)

que se realizan en: Enrique Cubero, 9, 47014 (Valladolid).

considerando las normas: ETSI EN 319 401; ETSI EN 319 421

Fecha de primera emisión: 2019-10-08
Fecha de modificación: 2020-11-30
Fecha de expiración: 2022-11-29

Este certificado solamente es válido en conjunción con Informe de Evaluación de Conformidad ("eIDAS Conformity Assessment Report 2019-0280-GEN-02 DIGITEL_202011-v0.5" de fecha 30 de Noviembre de 2020")

AENOR INTERNACIONAL, S.A.U
Génova, 6. 28004 Madrid. España
Tel. 91 432 60 00.- www.aenor.com

Rafael GARCÍA MEIRO
Director General

Bureau Veritas Certification

Certificación

Concedida a

DIGITEL ON TRUSTED SERVICES SLU

CL ENRIQUE CUBERO, 9 – 47014 – VALLADOLID – ESPAÑA

Bureau Veritas Certification certifica que el Sistema de Gestión ha sido auditado y encontrado conforme con los requisitos de la norma:

NORMA

ISO/IEC 27001:2013

El Sistema de Gestión se aplica a:

EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE DA SOPORTE A LOS SERVICIOS DE CONSULTORÍA, ACTIVIDADES TECNOLÓGICAS Y TRATAMIENTO DE ARCHIVOS Y CUSTODIA EN PROCESOS DE CONTRATACIÓN ELECTRÓNICA CERTIFICADA, SEGÚN LA DECLARACIÓN DE APLICABILIDAD DEL 15/11/2018.

Número del certificado: ES110314-1
Aprobación original: 29-06-2017
Certificado en vigor: 29-06-2020
Caducidad del certificado: 28-06-2023

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/Valportillo Primera 22-24, Edificio Caoba, 28108 Alcobendas – Madrid, España
t/t

1.2 Auditorías de Seguridad de la Información

Digitel TS planifica y elabora un **plan de Auditorías Internas y Externas** en materia de Seguridad de la Información, Protección de Datos de Carácter Personal (RGPD/LOPDGDD) y proveedor de servicios de confianza cualificados según reglamento eIDAS.

El **programa de auditorías** se resume a continuación:

- Auditorías internas anuales SGSI – 27001:2013
- Auditorías externas anuales SGSI – 27001:2013
- Auditorías internas anuales eIDAS
- Auditorías externas anuales - eIDAS
- Auditorias bianuales: LOPDGDD / RGPD

1.3 Áreas y departamentos

Contamos con las siguientes **áreas en Materia de seguridad.**

- CSSI - Comité de Seguridad de los Sistemas de Información
- CDataProtect - Comité de Protección de Datos
- SOC - Security Operations Center
- Departamento jurídico en materia de apoyo legal/normativo

1.4 Planes de Formación y Concienciación en Seguridad

Contamos con diversos **programas internos de formación y concienciación en Ciberseguridad y protección de Datos** con el objetivo de garantizar:

- Plan de formación en ciberseguridad
- Boletines internos de ciberseguridad mensuales
- Programa de concienciación en ciberseguridad / Simulación de ataques phishing.
- Conferencias divulgativas SharingNet.

1.5 Desarrollo Seguro, Privacidad y Seguridad desde el diseño

Digitel TS dispone en constante evolución de diferentes **políticas y procedimientos internos** (DOM-13 – Security And Privacy By design, PRO-12 – Procedimiento de Desarrollo Seguro) **y externos** (OWASP Security By Design Principles, OWASP Application Security Verification Standard) **de desarrollo seguro y de privacidad y seguridad** desde el diseño basados en diversas metodologías y estándares actuales.

1.6 Contratos, Acuerdos de confidencialidad, Normas de uso y Política de seguridad

Antes de tener acceso a ningún recurso, los empleados deben firmar el **contrato**, **Acuerdos de confidencialidad,** y leer y conocer el documento de **Normas de Uso y Protección de Datos,** el **Manual de Conducta**, así como las **políticas de Seguridad de la Información, Calidad o la documentación necesaria de Prevención de Riesgos Laborales.** Tras la recepción, lectura y comprensión de dichos documentos, el personal acepta digitalmente su cumplimiento.

Estos documentos están accesibles en todo momento, puesto que se encuentran en formato digitalizado y cualquier modificación en ellos es notificada, haciendo necesaria la aceptación de nuevo tras cualquier cambio.

1.7 Seguridad física y del entorno en las instalaciones

Disponemos de una **Política de Seguridad física y del entorno** la cual define y establece los mecanismos de implementados en todas las instalaciones que albergan Sistemas de Información, ya sean instalaciones propias, o instalaciones contratadas a través de proveedores, con el objetivo de prevenir accesos físicos no autorizados a las dependencias físicas y a los sistemas de la compañía y garantizar la protección y la privacidad de la información

Los **controles de acceso** a las áreas seguras **se basan en los siguientes mecanismos:**

- Gestión de acceso por huella.
- Gestión de acceso por llave.
- Personal de recepción y personal de seguridad.
- Sistema de Videovigilancia con grabación.

1.8 Seguridad del usuario y Puesto de trabajo

Aplicamos las siguientes medidas para garantizar una seguridad del usuario y del puesto de trabajo:

- **Accesos:** Todos los accesos son nominales y se gestionan mediante el Dominio Centralizado.
- **Gestión de accesos:** Se realiza por Políticas y Grupos de Dominio, que determinan los permisos de los usuarios bajo el principio del mínimo privilegio.
- **Antivirus, Antimalware, Anti-ransomware y Firewall:** Todas las estaciones de trabajo disponen de un Endpoint Antivirus, antimalware y Firewall. Tanto el software, y las bases de datos de firmas de antivirus se mantienen siempre actualizados.

  Dicho software es administrado de forma centralizada para la creación de alarmas, informes y correlación de eventos de seguridad.
- **EDR:** Todas las estaciones de trabajo disponen de EDR (Endpoint Detection and Response) centralizado para garantizar funciones avanzadas de análisis, detección, investigación y contención de las amenazas avanzadas.
- **Actualización de Sistema Operativos Centralizada:** Para mantener un nivel de seguridad mayor y evitar las vulnerabilidades, las actualizaciones de los Sistemas Operativos de gestionan de forma centralizada.
- **Auditoria de accesos:** La auditoría de accesos se realiza de forma periódica por las áreas de seguridad o bajo petición.

- **Equipo informático desatendido y bloqueo de pantalla:** Siempre que el empleado se ausente de su mesa de trabajo, aunque sea por una pausa mínima, debe bloquear su ordenador personal con el protector de pantalla del sistema operativo de forma que el desbloqueo vaya protegido con la contraseña del usuario.

  No obstante, el equipo se bloqueará de forma automática tras 300 segundos de inactividad en el equipo.

1.9 Compliance – RGPD, Comunicación de incidentes, Derechos de los interesados, EIPDs

Contamos con **políticas y procedimientos internos** en materia de Evaluaciones de Impacto, gestión y comunicación de incidentes de seguridad, atención a los derechos de los interesados, entre otros, para garantizar un **nivel de cumplimiento en materia de protección de datos.**

- **Reglamento General de Protección de Datos.**

Conocemos y aplicamos los artículos establecidos por el **Reglamento General de Protección de Datos (RGPD)** en todos los proyectos en los que se lleve a cabo tratamiento de Datos Personales.

http://www.privacy-regulation.eu/es/index.htm

- **Delegado de Protección de Datos**

En cumplimiento del **Artículo 37 del Reglamento General de Protección de Datos** ha designado un delegado de protección de datos, este nombramiento se ha realizado formalmente y comunicado a la autoridad de control.

Publicamos los datos de contacto del delegado de protección de datos a través de la política de privacidad publicada en la web corporativa.

https://privacidad.madisonmk.com/POLITICA_TELECYL

- **Derechos de los interesados**

En cumplimiento de **los Artículos 15 a 22 y 34 del RGPD, y 13 a 18 de LOPDGDD** garantiza el **Ejercicio de los derechos de los interesados** poniendo a su disposición mecanismos visibles, accesibles y sencillos que hagan posible cumplir con los plazos establecidos. En los tratamientos para los cuales Digitel TS es encargado, se comunicará al responsable las solicitudes recibidas por los interesados en los plazos establecidos.

https://privacidad.madisonmk.com/derechos

- **Notificación de brechas de seguridad**

En cumplimiento del **artículo 33 del RGDP** realizará la notificación de las **violaciones de Seguridad a la autoridad de control competente** en los plazos establecidos. En los tratamientos para los cuales Digitel TS encargado, comunicará sin dilación indebida al responsable del tratamiento las brechas de seguridad de los datos personales de las que tenga conocimiento.

- **Evaluaciones de Impacto relativa a la protección de datos (EIPD)**

El delegado de protección de datos, en colaboración con el Security Operations Center (SOC), realiza una Evaluación de Impacto relativa a la protección de datos (EIPD) sobre los tratamientos que así sean requeridos en base al **Artículo 35 del Reglamento General de Protección de Datos y sobre los Tratamientos** para los cuales Digitel TS sea encargado y requerido por el responsable en base a un Contrato u acto jurídico.

Para ello dispone de una herramienta para registro de tratamiento de datos, y evaluaciones de impacto, que permite **registrar, documentar y analizar el tratamiento de datos** que lleva a cabo un proyecto.