POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Aprobación y entrada en vigor

Texto aprobado el día 05 de mayo del 2026 por la Dirección.

Esta política de seguridad de la información está vigente desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Este texto deroga al anterior, que fue aprobado el 22 de octubre de 2025 por la Dirección.

2. Introducción

MIRA LO QUE TE DIGO, SLU, en adelante **MQD**, depende de la integridad y disponibilidad de sus sistemas de información para alcanzar sus objetivos de negocio. Esta Política de Seguridad de la Información establece el marco para proteger nuestros activos frente a amenazas accidentales o deliberadas.

Nuestro compromiso es garantizar que:

- La información sea veraz y accesible para quienes lo necesiten (disponibilidad e integridad).
- Los datos sensibles están protegidos contra accesos no autorizados (confidencialidad).
- Podamos identificar quién accede a qué y asegurar que cada acción es legítima (autenticidad y trazabilidad).
- La actividad no se detenga ante incidentes técnicos (continuidad).

La seguridad no es un parche posterior sino una parte integral de nuestros procesos. Aplicamos una estrategia de defensa en profundidad y gestión basada en el riesgo, asegurando que cada nuevo proyecto o sistema sea seguro desde su concepción hasta su retirada.

Como pilar de nuestra operativa, **MQD** adopta el Esquema Nacional de Seguridad (en adelante ENS) como estándar de referencia.

Esta Política se desarrolla mediante un cuerpo normativo, con normas, procedimientos e instrucciones de trabajo, cuya estructura y gestión se detallan en el Manual del Sistema.

3. Alcance

Esta política se aplica a todos los sistemas de información de **MQD**, a las personas que conforman la organización y a los prestadores de servicios o proveedores TIC de **MQD**.

4. Misión y objetivos de MQD

4.1. Misión

La misión de **MQD** es garantizar la accesibilidad universal a la información y la comunicación mediante la supresión de barreras sensoriales, asegurando la prestación ininterrumpida de servicios tecnológicos de apoyo a personas con discapacidad.

4.2. Servicios críticos bajo el alcance del ENS

Para el cumplimiento de la misión, **MQD** gestiona y protege activos de información que soportan los siguientes servicios:

- Subtitulado en directo
- Lengua de signos
- Interpretación simultánea
- Audiodescripción
- Transcripción
- Audio-signoguías
- Audiovisuales adaptados

4.3. Objetivos de seguridad

Para asegurar la continuidad de estos servicios y la confianza de nuestros clientes y usuarios, **MQD** establece los siguientes objetivos estratégicos de seguridad:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de **MQD** respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmitida a través de redes de comunicación sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. Principios de Seguridad de la Información

Los principios de Seguridad de la Información que rigen la actuación de **MQD** son:

- **Alcance estratégico**: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- **Seguridad integral**: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de la seguridad basada en el riesgo**: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- **Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes**, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- **Existencia de líneas de defensa**, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- **Vigilancia continua y reevaluación periódica**: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- **Seguridad por defecto y desde el diseño**: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- **Diferenciación de responsabilidades**, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6. Marco normativo

La actividad de **MQD** se desarrolla bajo un marco legal y reglamentario que garantiza la seguridad de la información y la protección de los derechos de los ciudadanos. La organización se compromete a cumplir con el Esquema Nacional de Seguridad (RD 311/2022, de 3 de mayo) y la normativa vigente de protección de datos personales. Como soporte para la implementación técnica de los controles, la organización adopta las Guías CCN-STIC como estándar de referencia oficial.

El detalle de la legislación y normativa sectorial, técnica y contractual aplicable se mantiene en un Inventario normativo, bajo responsabilidad del Responsable de Seguridad, siendo revisado al menos una vez al año o siempre que se produzcan cambios legislativos o normativos significativos, garantizando así la actualización constante del marco legal.

7. Organización de la seguridad de la información

La seguridad de la información en **MQD** se articula mediante una estructura de roles definidos que asegura la protección de los activos y la continuidad de los servicios. Siguiendo los principios del ENS, garantizamos que cada figura cuente con la autoridad necesaria para ejercer sus funciones, estableciendo mecanismos de supervisión mutua que aseguran la objetividad en la toma de decisiones.

En **MQD**, la gestión de la seguridad no es una responsabilidad aislada sino un compromiso coordinado entre los propietarios del negocio (Información y Servicio) y los responsables técnicos (Seguridad y Sistemas), bajo la supervisión del Comité de Seguridad.

La asignación de estos roles recaerá en las personas que ocupen los puestos correspondientes en cada momento. Los cambios significativos en la estructura organizativa que afecte a las responsabilidades sobre seguridad de la información, se comunicarán en el Comité de Seguridad de la Información y quedará reflejado en las actas del mismo.

7.1. Dirección

La Dirección ostenta la máxima responsabilidad en el desarrollo de las competencias de **MQD**, incluyendo las de seguridad de la información.

Sus funciones principales en materia de seguridad de la información son:

a. Aprobar la política de seguridad de la información.
b. Aprobar la política de protección de datos.
c. Nombrar al Responsable de Seguridad.
d. Facilitar los recursos adecuados para alcanzar los objetivos propuestos.
e. Responsable último del cumplimiento de las obligaciones en materia de seguridad.
f. Presidir el Comité de Seguridad.

7.2. Comité de Seguridad de la Información

Órgano colegiado que coordina la seguridad de la información en **MQD**.

Está formado por todas las personas que participan en la responsabilidad, definición o implantación de la ciberseguridad tratada y los servicios prestados:

- Dirección, como titular de **MQD**, ostentará la presidencia del Comité.
- Responsable de la Información.
- Responsables de los Servicios.
- Responsable de la Seguridad, actuará como secretario del Comité.
- Responsable del Sistema.
- Delegado de Protección de Datos, a través de su Punto de Contacto (POC).

Sus funciones principales son:

a. Atender las inquietudes sobre seguridad que Dirección o algún departamento plantee.
b. Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
c. Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.
d. Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
e. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información.
f. Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual, pudiendo proponer acciones de mejora.
g. Elaborar y revisar regularmente, la Política de Seguridad de la Información para su aprobación por Dirección y aprobar la Normativa de Seguridad de la información.
h. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
i. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
j. Velar porque se respete el principio de seguridad desde el diseño. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.
k. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables o entre diferentes áreas.

7.3. Responsable de la Información

Es la responsabilidad última de lo que se haga con la información y, por tanto, de su protección. En **MQD** queda asociado al rol de Dirección.

Es la figura que determina los niveles de seguridad de la información tratada, definiendo sus requisitos de confidencialidad, integridad y autenticidad. Como propietario de los datos, tiene la potestad última de validar y aceptar los riesgos residuales que afecten a la información bajo su responsabilidad.

Sus funciones principales son:

a. Determinar los requisitos de seguridad: definir, con el asesoramiento del Responsable de Seguridad, qué niveles de confidencialidad, integridad y autenticidad debe tener la información.
b. Clasificar la información: catalogar los activos de información según su criticidad para el negocio, indicando qué es público, qué es interno y qué es confidencial.
c. Valorar el impacto: evaluar, en el marco del análisis de riesgo, qué perjuicio supondría para **MQD** una pérdida de integridad o una filtración de los datos.
d. Aceptar los riesgos residuales: validar formalmente los riesgos que persistan tras la aplicación de medidas de seguridad, asumiendo la responsabilidad sobre el estado de la información.
e. Supervisar el acceso: definir quién tiene derecho a acceder a cada tipo de información, delegando la ejecución técnica en el Responsable del Sistema.
f. Participar en el Comité de Seguridad: aportar la visión de negocio en la toma de decisiones estratégicas sobre la protección de la información.

7.4. Responsable del Servicio

Es la figura que determina los requisitos de disponibilidad y continuidad de los servicios prestados por **MQD**. Su papel es asegurar que los sistemas de información den soporte efectivo a los procesos de negocio, definiendo los niveles de servicio necesarios para cumplir con los compromisos ante clientes y terceros.

Sus funciones principales son:

a. Determinar la disponibilidad: definir, con el apoyo del Responsable de Seguridad, el tiempo máximo que un servicio puede estar interrumpido y el nivel de pérdida de datos tolerable.
b. Establecer los requisitos de continuidad: identificar los procesos críticos de **MQD** que requieren planes de recuperación ante desastres para garantizar la actividad.
c. Valorar el impacto por interrupción: evaluar, dentro del análisis de riesgos, las consecuencias económicas, operativas o reputacionales de una caída del servicio.
d. Aceptar los riesgos de continuidad: validar y firmar los riesgos residuales relacionados con la disponibilidad, tras la implementación de las medidas propuestas por Seguridad y Sistemas.
e. Supervisar la entrega del servicio: asegurar que las medidas de seguridad implantadas no impidan o dificulten excesivamente la operatividad y el cumplimiento de los plazos de entrega de **MQD**.
f. Participar en el Comité de Seguridad: reportar las necesidades operativas de producción para que la estrategia de seguridad esté alineada con los objetivos de negocio.

7.5. Responsable de Seguridad de la Información

Es la figura encargada de determinar las decisiones tecnológicas y organizativas para asegurar que la información y los servicios cumplen con los requisitos de seguridad establecidos. Su función es actuar como nexo entre la estrategia de negocio y la implementación técnica, supervisando la eficacia de los controles y liderando la gestión de riesgos.

Dada su condición de responsable del Sistema de Gestión de la Seguridad de la Información (SGSI), es el garante del ciclo de mejora continua, liderando las revisiones por la dirección y los procesos de auditoría externa e interna.

Sus funciones principales son:

a. Determinar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
b. Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y los Servicios.
c. Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y los Servicios.
d. Liderar el análisis de riesgos
e. Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
f. Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación con el ENS.
g. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
h. Calificar la peligrosidad de los ciberincidentes y notificar a las autoridades cuando sea pertinente.
i. Colaborar con el Delegado de Protección de Datos o la Persona de Contacto (POC) en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.
j. Velar por que los proveedores y colaboradores externos cumplan con los niveles de seguridad aceptables.

k. Revisar periódicamente la eficacia de las medidas de seguridad y proponer cambios basados en la evolución de las amenazas.
l. Actuar como el interlocutor principal y responsable de coordinar las auditorías de certificación o cumplimiento del ENS, asegurando la provisión de evidencias y liderando la respuesta a las posibles no conformidades detectadas.
m. Participar en el Comité de Seguridad con funciones estratégicas como:
    - m.1. Informar periódicamente al Comité sobre el nivel de cumplimiento de la política y el estado de los controles.
    - m.2. Presentar los resultados del análisis de riesgos al Comité para que los Responsables de Información y de los Servicios validen las decisiones.
    - m.3. Identificar y proponer al Comité las necesidades de recursos (humanos, técnicos y económicos) para mantener el nivel de seguridad requerido.
    - m.4. Informar sobre el avance de los planes de mejora y las acciones correctivas derivadas de auditorías o incidentes.

Además, como secretario del Comité de Seguridad de la Información:

i. Convocar las reuniones según instrucciones del Presidente.
j. Preparar los temas a tratar.
k. Elaborar el acta de las reuniones.
l. Remitir el acta de las reuniones a los asistentes para conseguir su aceptación.
m. Conservar las actas.

7.6. Responsable del Sistema

Es la figura encargada de la implantación, gestión y mantenimiento operativo de las medidas de seguridad aplicadas a los sistemas de información. Su función es garantizar que la infraestructura tecnológica soporte los requisitos de seguridad definidos, ejecutando las configuraciones técnicas y los procedimientos operativos necesarios para la protección del sistema bajo la supervisión del Responsable de Seguridad.

Sus funciones principales son:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b. Adopción de las medidas correctoras derivadas de las auditorías de seguridad.
c. En ciberincidentes podrá, de acuerdo con el Responsable de Seguridad de la Información y avisando al Responsable del Servicio, suspender de forma cautelar y urgente el tratamiento de la información y prestación de los servicios como medida de contención.
d. Implementación, gestión y mantenimientos de las medidas de seguridad aplicables al sistema de información.
e. La gestión, configuración y actualización del HW y SW en los que se basa la seguridad del sistema de información.
f. La aplicación de los procedimientos operativos de seguridad.
g. Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
h. Colaborar con la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
i. Comprobar que los controles de seguridad establecidos son adecuadamente observados.
j. Comprobar que son aplicados los procedimientos de seguridad aprobados.
k. La gestión de las autorizaciones y privilegios concedidos a los usuarios, incluyendo la monitorización de los mismos.
l. Comprobar las instalaciones de HW y SW para asegurar que la seguridad no está comprometida y que se ajusta a las autorizaciones pertinentes.
m. Monitorizar el estado de seguridad del sistema.
n. Participar en el Comité de Seguridad para proporcionar asesoramiento técnico sobre la infraestructura y el estado de implantación de las medidas.

8. Tratamiento de datos personales

MQD trata datos de carácter personal limitados principalmente a la gestión administrativa, laboral y de contacto profesional necesaria para su funcionamiento, tal y como se detalla en su Registro de Actividades de Tratamiento.

8.1. Cumplimiento normativo

MQD cumple con el Reglamento General de Protección de Datos (RGPD) y la normativa nacional vigente. La información detallada sobre estos tratamientos es accesible a través de nuestra Política de Privacidad: https://www.mqd.es/politica-privacidad/

8.2. Integración de la seguridad

Las medidas de seguridad aplicadas a los datos personales están integradas en el marco global de seguridad del ENS. El análisis de riesgos de seguridad tendrá en cuenta la protección de la privacidad, coordinando medidas técnicas con el Delegado de Protección de Datos (o a través del Punto de Contacto, POC).

8.3. Gestión de brechas de seguridad

En caso de producirse un incidente que afecte a datos personales, el Responsable de Seguridad coordinará la respuesta con el responsable de la privacidad para cumplir con las obligaciones de notificación a las autoridades y a los interesados, si fuera necesario.

8.4. Evaluación de riesgos

El análisis de riesgos de los sistemas que dan soporte a datos personales se revisará periódicamente o cuando existan cambios significativos en los tratamientos, asegurando que el nivel de protección técnica sea coherente con la sensibilidad de los datos.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para garantizar la coherencia en la gestión de riesgos, el Responsable de Seguridad centralizará los criterios comunes de valoración de activos. Así mismo, se priorizará la adquisición de herramientas de seguridad transversales que aseguren un control uniforme en toda la organización, optimizando los recursos disponibles.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos (o a través del Punto de Contacto, POC) y se coordinarán los planes del tratamiento del riesgo.

10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad es pública y está a disposición de todos los miembros de la organización y partes interesadas.

La normativa técnica, instrucciones y procedimientos que desarrollan esta Política tienen carácter restringido. El personal con funciones de operación o administración de sistemas accederá a dichos documentos según su perfil de acceso y responsabilidades, a través de los canales de comunicación interna autorizados por el Responsable de Seguridad.

11. Obligaciones del personal

Todos los miembros de **MQD** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad del Responsable de Seguridad de la Información, apoyándose en el área de personal, de disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **MQD** atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **MQD**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo

12. Relación con terceros

Para garantizar la seguridad de la información en toda la cadena de suministro, se establecen las siguientes directrices:

- Cumplimiento contractual: todo proveedor que trate información de la organización o acceda a sus sistemas deberá adherirse por contrato a esta Política y a los requisitos del ENS o estándares equivalentes.
- Gestión de riesgos: si un proveedor no puede cumplir con algún requisito de seguridad, el Responsable de Seguridad deberá evaluar el riesgo y la Dirección deberá aceptarlo formalmente antes de la contratación.
- Supervisor y auditoría: la organización se reserva el derecho de solicitar evidencias de cumplimiento, informes de auditoría o realizar supervisiones periódicas a los proveedores críticos.
- Punto de Contacto (POC): Se establecerán canales de comunicación específicos para el reporte de incidentes. En caso de afectación a datos personales, se coordinará directamente con el Delegado de Protección de Datos.
- Inteligencia Artificial: la implementación de sistemas de IA requerirá un análisis de seguridad previo que evalúe el impacto en la protección de datos y la integridad del sistema.

13. Gestión de incidentes de seguridad

MQD garantiza la capacidad de respuesta ante eventos que comprometan la seguridad de la información mediante las siguientes directrices:

- Procedimiento de respuesta ante incidentes: se dispone de un protocolo operativo para la detección, notificación, registro y resolución de incidentes, orientado a minimizar el impacto y recuperar los servicios en el menor tiempo posible.
- Notificación obligatoria: todo empleado o tercero que detecte una anomalía debe reportarla de inmediato al Responsable de Seguridad por los canales establecidos.
- Coordinación y cumplimiento legal: ante incidentes que afecten a datos de carácter personal, se activará la comunicación con el DPD para cumplir con la notificación a la AEPD en un plazo máximo de 72 horas, cuando así esté requerido.
- Colaboración externa: cuando la gravedad del incidente lo requiera (delitos informáticos, ataques dirigidos o impacto crítico), el Responsable de Seguridad coordinará la comunicación con el CCN-CERT, las Fuerzas y Cuerpos de Seguridad o las autoridades judiciales competentes.

14. Aprobación de la Política y entrada en vigor

La presente Política de Seguridad de la Información estará sujeta a un ciclo de revisión y actualización permanente para garantizar su eficacia y alineación con los objetivos de **MQD**.

El Comité de Seguridad de la Información revisará esta Política con carácter anual o siempre que se produzca un cambio significativo en la infraestructura, los servicios prestados o el marco normativo (ENS / RGPD).

El Responsable de Seguridad de la Información es el encargado de detectar ineficiencias y proponer las modificaciones necesarias. El Comité de Seguridad analizará y elaborará las propuestas de actualización. La Dirección, como autoridad máxima y presidencia del Comité, es la única figura competente para la aprobación formal de la Política y sus versiones sucesivas.

Las modificaciones entrarán en vigor de forma inmediata tras la ratificación por parte de la Dirección.

Una vez aprobada, la nueva versión será comunicada a todo el personal y partes interesadas. El Responsable de Seguridad velará por que la versión vigente sea la única accesible, retirando las versiones obsoletas para garantizar la integridad del sistema documental.

Burgos, a 5 de mayo de 2026

La Dirección

Firmado digitalmente por 71265985W RAUL TOTORICA (R: B09367657)
Fecha: 2026.05.27 10:44:40 +02'00'