POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo.

1.1. La Política de Seguridad de la Información de **MIRA LO QUE TE DIGO, S.L.U.**, (en adelante, **MQD**), identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

1.2. La Política de Seguridad de la Información es el instrumento en que se apoya **MQD** para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones.

1.3. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en **MQD**.

2. Alcance.

2.1. La Política de Seguridad de la Información será de obligado cumplimiento para todos los organismos participativos y directivos de **MQD**, así como para terceras partes a las que **MQD** preste servicios, cedan información, o de las que utilicen servicios o manejen información.

2.2. La Política de Seguridad de la Información estará disponible en la página web corporativa https://www.mqd.es/.

3. Marco normativo.

El marco normativo de las actividades de **MQD** en el ámbito de la Política de Seguridad de la Información está integrado por las siguientes normas:

a) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
b) 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 y por el que se deroga la Directiva 95/46/CE.
c) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
d) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
e) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
f) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
g) Ley 59/2003, de 19 de diciembre, de firma electrónica.
h) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
i) Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
j) Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
k) Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
l) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
m) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
n) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
o) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica.

4. Principios y directrices.

4.1. Los principios y directrices que deben de contemplarse a la hora de garantizar la seguridad de la información y asegurar que **MQD** cumpla sus objetivos utilizando sistemas de información, son los que se establecen en las siguientes normas:

a) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica.
b) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y su reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante, RLOPD).
c) 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.

4.2. Principios y directrices en la Política de Seguridad de la Información.

4.2.1. 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 información.

4.2.2. Gestión de riesgos. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

4.2.3. Prevención, reacción y recuperación. La seguridad del sistema debe contemplar aspectos de prevención, detección, respuesta y recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan. **MQD** debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, sus órganos directivos deben implementar las medidas mínimas de seguridad determinadas por el ENS y por el RLOPD para tratamientos automatizados. Así mismo deberán tenerse en cuenta las medidas especificadas en el artículo 32 del Reglamento UE 2016/679, que deberán garantizar un nivel de seguridad adecuado al riesgo para tratamientos automatizados, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, en particular:

a) Para garantizar el cumplimiento de la Política de Seguridad de la Información, los órganos directivos responsables deben:
- Autorizar los sistemas o los servicios antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica del cumplimiento del ENS por parte de terceros.

b) Dado que los sistemas y servicios pueden degradarse rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS. En el supuesto de que la degradación sea atribuida a incidentes de seguridad, los órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.
c) Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad. Con el fin de garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4.2.4. Líneas de defensa. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

- Ganar tiempo para una reacción adecuada.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

4.2.5. Reevaluación periódica. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

4.2.6. La seguridad como función diferenciada. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, siendo el Responsable de la Información quien determinará los requisitos de la información tratada, el Responsable del Servicio quien determinará los requisitos de los servicios prestados, y el Responsable de Seguridad quien determinará las decisiones técnicas para satisfacer los requisitos de seguridad de la información y de los servicios.

5. Estructura.

5.1. La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel: Política de Seguridad de la Información.
b) Segundo nivel: Manual del Sistema.
c) Tercer nivel: Fichas de proceso de Seguridad de la Información.
d) Cuarto nivel: Instrucciones de Seguridad de la Información.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de **MQD**, sin necesidad de revisar su estrategia de seguridad.

5.2. El personal de **MQD** tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones. La Política, las Instrucciones y los Procedimientos de Seguridad de la información estarán disponibles en la aplicación de soporte al sistema TQNET (tqnet.teqnoquality.com).

5.3. Niveles de la Política de Seguridad de la Información:

5.3.1. Primer nivel: Política de Seguridad de la Información. Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto y aprobada por la Junta Directiva.

5.3.2. Segundo nivel: Manual del Sistema. El segundo nivel desarrolla la Política de Seguridad de la Información y establece una relación directa entre los apartados del ENS y los documentos desarrollados como respuesta (metodología y evidencias de cumplimiento).

5.3.3. Tercer nivel: Fichas de Proceso de Seguridad de la Información. El tercer nivel desarrolla el Manual del Sistema mediante la definición de tareas específicas que abarcan un área o aspecto determinado de la seguridad de la información. Desarrollarán, al menos las siguientes materias:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.
b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.
c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información.

h) Gestión de los incidentes de seguridad implantando los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
i) Gestión de la continuidad implantando los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

5.3.4. Cuarto nivel: Instrucciones de Seguridad de la Información. El cuarto nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobadas por el Responsable de Seguridad de la Información o por los Responsables de la Información o los de los Servicios, según su ámbito de competencia. Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

6. Organización de la seguridad.

La organización de la seguridad en **MQD** queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

6.1. Junta Directiva.

6.1.1. La Junta Directiva de **MQD**, mediante la aprobación del presente Acuerdo, asegura el compromiso de las autoridades de **MQD** en la aplicación del ENS.

6.1.2. Este compromiso se manifiesta mediante la aprobación de la Política de Seguridad de la Información, así como de todas aquellas modificaciones o actualizaciones de la misma que el Comité de Seguridad de la Información pueda proponer, en el ámbito de sus competencias.

6.2. Comité de Seguridad de la Información. Se trata de un comité de carácter interdepartamental, adjunto a la Consejera Delegada. La coordinación que se pretende con la creación del Comité se orienta a asegurar el carácter armónico e integrador de todas las actuaciones en materia de tecnologías de la información y comunicaciones de la organización, facilitando las actuaciones conjuntas de los diversos órganos afectados.

6.3. Responsable de Seguridad de la Información.

6.3.1. Corresponde a la persona titular del puesto de Director Técnico, según el organigrama de **MQD**, establecer las medidas necesarias para cumplir los requisitos de seguridad establecidos por los responsables de la información y de los servicios manejados por el sistema.

6.3.2. En el ejercicio de las citadas competencias, el Responsable de Seguridad de la Información desarrollará las siguientes funciones:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Analizar y elevar al Comité de Seguridad de la Información toda la documentación relacionada con las instrucciones de seguridad de la información para su aprobación.
c) Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.
d) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
e) Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.
f) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
g) Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

6.4. Responsables de la Información.

6.4.1. Son responsables de la Información los titulares de los perfiles de Responsable de cada Servicio responsables a su vez de la información afectada por la presente Política de Seguridad de la Información, en sus respectivos ámbitos de competencia.

6.4.2. Corresponde a los Responsables de la Información establecer los requisitos de la información en materia de seguridad, y en particular:

a) Determinar los niveles de seguridad de la información tratada y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
b) Realizar, junto a los Responsables del Servicio y el Responsable de Seguridad de la Información, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
c) Aceptar los riesgos residuales respecto de la información calculada en el análisis de riesgos.
d) Realizar el seguimiento y control de los riesgos.

6.5. Responsables del Servicio.

6.5.1. Son Responsables del Servicio los responsables de cada servicio prestado por la organización afecto a la presente Política de Seguridad de la Información, en sus respectivos ámbitos de competencia.

6.5.2. Corresponde a los Responsables del Servicio establecer los requisitos del servicio en materia de seguridad, y en particular:

a) Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
b) Realizar, junto a los Responsables de la Información y el Responsable de Seguridad de la Información, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se deban implantar.
c) Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
d) Realizar el seguimiento y control de los riesgos.
e) Suspender, de acuerdo con los Responsables de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

6.6. Resolución de conflictos.

6.6.1. En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el Comité de la Seguridad de la Información o por la Consejera Delegada en última instancia.

6.6.2. En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

7. Datos de carácter personal.

7.1. **MQD** realiza tratamientos de datos de carácter personal. La política de privacidad y de datos personales de la organización se encuentra publicada en la página corporativa https://www.mqd.es/politica-de-privacidad/.

7.2. Todos los sistemas de información de **MQD** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal detallados en su correspondiente Documento de Seguridad, de acuerdo con lo exigido por el RLOPD.

7.3. Corresponde al Director Técnico de la organización implementar las medidas de seguridad TIC exigidas por la normativa de protección de datos de carácter personal para tratamientos automatizados, definidas en el documento de seguridad correspondiente, y coordinadas y controladas por el responsable de seguridad de los datos personales de que se trate.

8. Concienciación y formación.

8.1. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

8.2. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos. El personal de **MQD** recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

8.3. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

9. Gestión de riesgos.

9.1. El análisis y gestión de riesgos, evaluando las amenazas y los riesgos a los que están expuestos la información, los servicios y sistemas de **MQD**, será la base para determinar las medidas de seguridad que se deben adoptar.

9.2. El análisis de riesgos se realizará:

a) Regularmente, al menos una vez al año.
b) Cuando cambie la información manejada.
c) Cuando cambien los servicios prestados.
d) Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.
e) Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del Real Decreto 3/2010, de 8 de enero.

9.3. Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información, asimismo, dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. Terceras partes.

10.1. Cuando **MQD** utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité de Seguridad de la Información establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

10.2. Cuando **MQD** preste servicios a otros organismos o ceda información a terceros, les hará partícipes de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información, quedando sujetos a las obligaciones que en ellos se establezcan, sin perjuicio de que puedan desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias y se exigirá que el personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. Tratándose de cesiones o comunicaciones de datos de carácter personal a terceros, aun cuando sean Administraciones Públicas, se estará a lo dispuesto en la LOPD, requiriéndose que la concienciación

se realice también en lo relativo al adecuado cumplimiento de la normativa sobre protección de datos de carácter personal.

10.3. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, de conformidad con lo dispuesto en los párrafos anteriores, será necesario que el Responsable de Seguridad emita un informe en el que se precisen los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los Responsables de la Información y los Servicios afectados para poder continuar con la utilización del servicio o el manejo de la información.

11. Revisión.

El Comité de Seguridad de la Información revisará anualmente la Política de Seguridad de la Información o cuando exista un cambio significativo que obligue a ello. La revisión será aprobada por la Junta Directiva de **MQD** y difundida para que la conozcan todas las partes afectadas.

Burgos, a 26 de marzo de 2021

La Junta Directiva

13161944X MARTA MERINO (R: B09367657)

Firmado digitalmente por 13161944X MARTA MERINO (R: B09367657)
Nombre de reconocimiento (DN): 2.5.4.13=Ref:AEAT/AEAT0432/PUESTO 1/68778/30062021090834, serialNumber=IDCES-13161944X, givenName=MARTA, sn=MERINO TOME, cn=13161944X MARTA MERINO (R: B09367657), 2.5.4.97=VATES-B09367657, o=MIRA LO QUE TE DIGO SL, c=ES
Fecha: 2021.11.19 10:42:48 +01'00'