CONTROL DE LA DOCUMENTACIÓN

CLASIFICACIÓN			
☐	Público	☐	Confidencial
☑	Interno	☐	Uso Oficial
☐	Restringido		

INTERNO

informática responsable®

POLÍTICA DE SEGURIDAD MR

INTERNO

INDICE

INTERNO

1 ALCANCE

Sistemas de información que proporcionan apoyo interno a los servicios prestados por MRInformática consistentes en la gestión de proyectos, servicios de auditoría y consultoría de procesos, sistemas y seguridad y servicios prestados en modo de asistencias técnicas realizadas sobre los propios sistemas del cliente.

MR INFORMÁTICA (en adelante MR), es una empresa consultora en Tecnologías de la Información, fundada en 1.995 por profesionales con amplia experiencia en el sector público. Nuestra actividad se centra fundamentalmente en la Administración Pública. Nuestra misión fundamental es evolucionar con nuestros clientes, facilitándoles la tecnología más apropiada para el desarrollo de su actividad.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

2 MARCO NORMATIVO

Esta política se enmarca en la siguiente legislación:

- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ENS Artículo 12. Organización e implantación del proceso de seguridad
- 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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
    - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Guía de Seguridad de las TIC CCN-STIC 805 ENS. Política de seguridad de la información.
- Guía de Seguridad de las TIC CCN-STIC 801 ENS. Responsabilidades y funciones.

INTERNO

- El convenio colectivo aplicable, correspondiente a “Empresas de consultoría, y estudios de mercado y de la opinión pública”.
- UNE-EN-ISO 9001, UNE-EN_ISO_14001, UNE-ISO-IEC_27001, UNE ISO 20000, CMMI v 2.0_DEV nivel 2 & SVC Nivel 3
- La Directiva 2022/2555 del Parlamento Europeo y del Consejo, conocida como NIS2

3 MISIÓN

El propósito de esta Política de Seguridad de la Información es proteger la información es establecer el conjunto de directrices que rigen la forma en que MR gestiona y protege la información que trata y los servicios que presta.

La política de Seguridad junto con la Normativa de Seguridad se realizará mediante una comunicación a todos los trabajadores, para que se efectúe el análisis, comprensión y lectura del documento.

Esta política aplica a Sistema de información propiedad de MR , para la adecuada prestación de los servicios de asistencia técnica, mediante la asignación de personal cualificado a organizaciones públicas, llevando a cabo su gestión y seguimiento en los ámbitos de:

- Asistencia técnica para el soporte a sistemas.
- Asistencia técnica para la atención y soporte a usuarios (Helpdesk).
- Asimismo, realización de consultoría TIC y de seguridad, junto a auditorías técnicas y de cumplimiento, todo ello según las disposiciones del RD 311/2022, ISO/IEC 27001 y la Declaración de Aplicabilidad vigente.

4 FUNCIONES DE SEGURIDAD

MR ha nombrado un COMITÉ de Seguridad con sus Funciones y Responsabilidades.
El establecimiento de este comité, así como la designación de los diferentes roles se hallan registrados en el Acta de Constitución del comité: MRSGAR248 de fecha 11/06/2021 y en Acta de Nombramientos: MRSGAR239 de fecha 11/06/2021

INTERNO

El Comité de Seguridad de la Información del ENS está formado por:

*Responsable de Seguridad.
*Responsable de Sistemas.
*Responsable de la Información.
*Responsable del Servicio.
*Responsable de Dirección .

Se deben identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de MR. Se detallarán en la política de seguridad de la organización las atribuciones de cada responsable.

Los nombramientos los establece la Dirección de MR y se revisan cada 2 años o cuando un puesto queda vacante o se produzca algún cambio significativo. Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

Los diferentes roles junto con sus respectivas funciones y responsabilidades:

El **Responsable de la Información** tendrá como funciones:

- Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Determinar los requisitos de la información tratada.
- Velar por la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad.
- Estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a MR.
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El **Responsable del servicio** tendrá las funciones:

- Determinar los requisitos de Seguridad de los servicios prestados en los Clientes.
- Revisar y aprobar los niveles de seguridad de los servicios.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios, se efectuará atendiendo a su repercusión en la capacidad de la MRInformática para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los Clientes.
- Asumir la propiedad de los riesgos sobre los servicios.

El **Responsable del sistema** tendrá las funciones:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema y determinar las medidas de seguridad que deben aplicarse Elaborar y aprobar la documentación de seguridad del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutado.

El **Responsable de seguridad** tendrá las funciones:

- Responsable de la Seguridad es la persona designada por la Dirección de la MR.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Trabajar para conseguir una total seguridad de los datos de la empresa, así como la privacidad de estos.
- Supervisar, controlar y administrar el acceso a la información de la empresa, y de sus trabajadores.
- Elaborar un conjunto de medidas de respuesta ante incidentes de seguridad relacionados con la información, incluyendo la recuperación ante desastres.
- Garantizar el cumplimiento de la normativa relacionada con la seguridad de la información.
- En caso de servicios externalizados, la responsabilidad última la tiene siempre la MR destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato) a la organización prestataria del servicio.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la MR.
- Promover la formación y concienciación en materia de seguridad de la información.
- Garantizar el buen uso del equipamiento informático dentro de su ámbito de responsabilidad.
- Supervisar y coordinar al equipo encargado de llevar a cabo las medidas de respuesta en caso de brechas de seguridad.
- POC (Persona de contacto de seguridad de la información) Se responsabilizará de la seguridad con los Clientes, en los que presta servicio MR.
- Realizar operaciones de seguridad para luchar contra el fraude y el robo de información.
- Diseñar del Plan de formación, en el ámbito del ENS, para las personas de MR que prestan servicios en proyectos de AA.PP.

INTERNO

- Realizar funciones de DPD: prestando la debida atención a los riesgos asociados a las operaciones de tratamiento teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Y cooperar con la autoridad de control.

El **Responsable de Dirección** tendrá las funciones:

- Es el encargado de definir las medidas a tomar para proteger los intereses de MR.
- Organizar el desarrollo de la organización preventiva de la empresa defiendo las funciones y responsabilidades correspondientes.

5 REPORTES

El administrador de seguridad reporta al Responsable del Sistema o al Responsable de la Seguridad, según sea su dependencia funcional:

- Incidentes relativos a la seguridad del sistema o acciones de configuración, actualización o corrección.
- El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- El Responsable del Sistema reporta al Responsable de la Seguridad:
  -Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema
  -Resumen consolidado de los incidentes de seguridad.

6 ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD (ART. 13)

Esta “Política de Seguridad de la Información” es efectiva desde su entrada en vigor el día 18 de febrero de 2023 por MR.

La Política es revisada por el Responsable de Seguridad de la Información a intervalos planificados, sin exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

INTERNO

La seguridad de los sistemas de información deberá comprometer a todos los miembros de de MR, comunicándose de forma efectiva.

Los cambios sobre la Política de Seguridad de la Información serán aprobados por la Dirección de MR. Cualquier cambio sobre la misma deberá ser difundido para conocimiento de toda MR.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

7 ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART. 14)

Se realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos según lo previsto en el artículo 7 y 14 del BOE, se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando haya un incidente de seguridad relacionado con la normativa LOPDGDD
- Cuando haya una brecha de seguridad relacionada con la información tratada de un usuario según la normativa LOPDGDD.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará MR, basándose en estándares y buenas prácticas reconocidas.
Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de MR de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios, o repercuta a dicha información tratada durante el servicio.

El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

8 GESTIÓN DE PERSONAL (ART. 15)

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en el documento Normativa de Seguridad que será aprobada por la dirección de MR. Se difundirá a toda la MR, siendo obligatoria su difusión para cada incorporación en MR.

9 PROFESIONALIDAD (ART. 16)

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

MR determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

10 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS (ART. 17)

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los privilegios de acceso de un recurso (persona) al sistema de información de MR, quedan restringidos por defecto al mínimo necesario para el desarrollo de sus funciones.

El sistema de información de MR se mantendrá siempre configurado, de tal manera que evite que un recurso (persona) pueda acceder accidentalmente a recursos con derechos distintos de los autorizados.

11 PROTECCIÓN DE LAS INSTALACIONES (ART. 18)

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de accesos adecuados y proporcionales en función del análisis de riesgos.

12 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD (ART. 19)

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición por el CCN-CERT o por otros Organismos internacionales reconocidos por el propio CCN.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

13 MÍNIMO PRIVILEGIO (ART. 20)

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la MR alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

14 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA (ART. 21)

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

15 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO (ART. 22)

En la MR e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida

con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

16 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS (ART. 23)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

17 REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO (ART. 24)

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

18 INCIDENTES DE SEGURIDAD (ART. 25)

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

19 CONTINUIDAD DE LA ACTIVIDAD (ART. 26)

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

20 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD (ART. 27)

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

.

CONTROL DE LA DISTRIBUCIÓN

COPIA	NOMBRE	PUESTO	ORGANIZACIÓN
1			MR

REGISTRO DE CAMBIOS

CÓDIGO	FECHA	PÁGINAS AFECTADAS	RAZONES DEL CAMBIO
MRSGPG012.02	04/04/2018	Todas	Versión con formato antiguo MR
MRSGPG012.03	30/06/2019	Todas	Revisión y actualización al RGPD. Versión con formato nuevo.
MRSGPG012.04	26/10/2020	Todas	Inclusión de Objetivos del ENS, y actualización con directrices del ENS
MRSGPG012.05	11/02/2021	Todas	Reestructuración y actualización de la Política de Seguridad del ENS
MRSGPG012.06	23/07/2021	Todas	Revisión y corrección de errores en los integrantes del Comité de Seguridad
MRSGPG012.07	10/11/2021	Todas	Inclusión de medida de seguridad 2FA
MRSGPG012.08	18/02/2023	Todas	Revisión y adaptación al nuevo ENS de RD 311/2022
MRSGPG012.09	25/07/2023	Todas	Insertado Marca de Água e índice.Cambios en el Índice agrupando los requisitos mínimos y principios básicos.Reorganización en el Marco Normativo: 1º los puntos de obligado cumplimiento y 2º los puntos de buenas prácticas. Inclusión del rol de Responsable de Dirección. Inclusión en distintos párrafos de artículos relacionados del ENS , RD 311/2022. Inclusión del rol de Responsable de Dirección.

INTERNO

INMRSGPG012.05	04/09/2024	Página 5	Incorporación de la normativa NIS2

	NOMBRE/PUESTO	FECHA
REALIZADO	Juan Manuel Rodríguez	04/09/2024
APROBADO	Maite del Río	04/09/2024

RODRIGUEZ ORTIZ JUAN MANUEL - 53104680A

Firmado digitalmente por RODRIGUEZ ORTIZ JUAN MANUEL - 53104680A
Fecha: 2024.09.26 17:19:12 +02'00'

Firmado por ***3469** MARIA TERESA DEL RIO (R: ****3025*) el día 27/09/2024 con un certificado emitido por AC Representación

INTERNO