POLÍTICA DE SEGURIDAD MR ENS

C/ Cea Bermúdez, 14 A 1º, 28003 Madrid
Telf. 91 534 00 76
www.mrinformatica.es

ÍNDICE

1 MISIÓN Y ALCANCE

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.

Esta política aplica a Sistema de información propiedad de MR Informática, 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 3/2010 y la Declaración de Aplicabilidad vigente.

2 MARCO NORMATIVO

2.1 IDENTIFICACIÓN

MR se encuentra sujeto a la siguiente normativa en la provisión de los Servicios prestados a sus clientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- RD 3/2010, de 8 de enero, 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.

- El convenio colectivo aplicable, correspondiente a "Empresas de consultoría, y estudios de mercado y de la opinión pública".
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- UNE-EN-ISO 9001, UNE-EN_ISO_14001, UNE-ISO-IEC_27001, UNE ISO 20000, CMMI_DEV&SVC_L2_v1.3.

2.2 DATOS DE CARÁCTER PERSONAL

El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de MR se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

3 PRINCIPIOS Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 4 del RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 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.

3.1 Prevención

Evita que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello MR tienen implementadas las medidas mínimas de Seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados. Para garantizar el cumplimiento de la política, de Seguridad de MR:

- Autoriza los sistemas antes de entrar en operación.

• Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, los servicios monitorizan 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. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Están establecidos mecanismos de detección, análisis y reporte, que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros preestablecidos como normales.

3.3 Respuesta

Se dispone de mecanismos para responder eficazmente a los incidentes de seguridad. El punto de contacto para las comunicaciones con respecto a incidentes a través de tickets abiertos en la herramienta correspondiente, por parte del responsable de Seguridad. El protocolo para el intercambio de información relacionada con el incidente se establece por medio del procedimiento Gestión de incidentes de seguridad de la Información".

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, MR dispone de un plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Se realizará un análisis de riesgos de todos los activos sujetos al alcance del ENS, evaluando las amenazas y los riesgos a los que están expuestos.

Este análisis 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

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 dinamizará la

disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

• La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que están adecuadamente formadas y concienciadas.

• La Seguridad de la Información no es algo estático, está constantemente controlada y periódicamente revisada.

• Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

• El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

4 ORGANIZACIÓN DE LA 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

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

*Responsable de Seguridad
*Responsable de Gestión
*Responsable de Dirección

Además existen los roles:

*Responsable de la Información
*Responsable de Sistemas
*Responsable del Servicio

4.1 Roles y responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en la en el documento: MRSGDI006._Perfiles y competencias de MR. Se ha tenido en cuenta lo dispuesto en la Guía de Seguridad de las TIC CCN-STIC 801 – Responsabilidades y Funciones.

4.2 Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección que podrá delegar en el Comité del SGI. Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante. Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité del SGI y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

5 FORMACIÓN Y CONCIENCIACIÓN

Todos los miembros de MR, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de MR, asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

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.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información
Que afecta a todos los miembros de MR dentro del alcance, de acuerdo al
Artículo 5 del ENS, así como la concienciación y Formación para conozcan los riesgos a los que se exponen.

6 GESTIÓN DE RIESGOS

Una correcta identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información, que sustentan los servicios de MR, es primordial para la correcta toma de decisiones de la Dirección. Esto ha motivado basar la Metodología de Análisis y Gestión de Riesgos del ENS en MAGERIT, metodología de apreciación del riesgo.

7 DOCUMENTACIÓN

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el procedimiento MR01MA01_PR control documentación, MR81PR029_Guia redacción de la documentación.

La responsabilidad de aprobación de los documentos será competencia de la Dirección de MR.

Informes, registros y evidencias electrónicas, documentos de carácter técnico que recogen evidencias generadas durante todas las fases del ciclo de vida del sistema de información, así como amenazas y vulnerabilidades de los sistemas de información.

Se podrán seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC que publique el Centro Criptológico Nacional (CCN)

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo a los requisitos generales del Sistema de Gestión Integrado que se recogen en el procedimiento interno “Manual de calidad”.

8 PROCESO DE APROBACIÓN Y REVISIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será misión del Responsable de Seguridad, difundirla para que la conozcan todas las personas de la organización.

Esta Política de Seguridad de la Información ENS es revisada junto a las demás Políticas de los Sistemas de Gestión de forma anual, o cuando las circunstancias técnicas u organizativas lo requieran.

9 RESOLUCIÓN DE CONFLICTOS

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 del Responsable de mayor rango: Responsable de Seguridad de MR.

10 DATOS DE CARÁCTER PERSONAL

El documento de seguridad, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de MR se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

11 OBJETIVOS DEL ENS

La Dirección de MR ha establecido un marco adecuado para la consecución de los objetivos de seguridad de la información.

Los objetivos generales establecidos en el marco del ENS y de la Norma ISO 27001, son los siguientes:

.

- ✓ MR, garantizará la seguridad de sus datos, actualmente en alojamiento externo, los sistemas y las comunicaciones que permita el funcionamiento correcto de la Organización y así mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio
- ✓ La gestión de la Seguridad será una labor permanente en la Organización, y en los servicios que preste en la AA.PP.
- ✓ Se emplearán las mejores prácticas, para el análisis de riesgos de los activos de la Organización. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
- ✓ MR, utilizará todos los medios de seguridad, para la detección de ciberataques y ciberamenazas, y su corrección en caso de que se produzcan.

12 TERCERAS PARTES

Cuando MR, preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política

Firma de Maite del Río – Dirección General

Firma de Juan Manuel Rodríguez - Responsable de Seguridad

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, de la política de Seguridad
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.
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

CONTROL DE LA DOCUMENTACIÓN

CLASIFICACIÓN			
☐	Público	☑	Interno
☐	Exclusivo uso por Cliente	☐	Confidencial

	NOMBRE/PUESTO	VALIDADO/FIRMA
REALIZADO	Mª Ángeles Gómez	23/07/2021
REVISADO y APROBADO	Maite del Río	23/07/2021