MNEMO

Políticas de Calidad, Seguridad y Medioambiente

v.1.3

Consideraciones de seguridad

La presente documentación es propiedad de MNEMO y tiene carácter de USO PÚBLICO. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro.

Asimismo, tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de MNEMO, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme dicte la ley.

Información del documento

Documento	Políticas de Calidad, Seguridad y Medioambiente		
Autor/es	Departamento de Calidad, Seguridad y Medioambiente		
Revisado por	Comité de Calidad, Seguridad y Medioambiente		
Aprobado por	Comité de Calidad, Seguridad y Medioambiente		
Fecha aprobación	13/05/2020	Fecha de implantación	13/05/2020

Historial de cambios

Fecha	Descripción	Realizado por	Versión
22/04/2020	Versión Inicial	CSMA	v.1.0
19/10/2020	Modificación de la política de Seguridad.	CSMA	v.1.1
12/11/2020	Modificación de las políticas de Seguridad, Continuidad y Servicio	CSMA	v.1.2
10/06/2021	Integración de políticas Calidad, Medioambiente y Seguridad de la información. Eliminación de política HLS. Separación de política de seguridad específica para ENS	CSMA	v.1.3

Índice

1. Política de Calidad, Medioambiente y Seguridad de la Información

El objetivo de **Grupo Mnemo** es acompañar a nuestros clientes en la obtención de sus objetivos de desarrollo empresarial a través de la prestación de servicios de consultoría en el mundo de las tecnologías de la información y de la comunicación.

Para cumplir con este objetivo, Grupo Mnemo ha desarrollado esta política integrada, conforme los estándares **ISO 9001:2015, 14001:2015 y 27001:2014** así como a la legislación aplicable, cuyo fin es asegurar que entendemos y compartimos las necesidades y expectativas de nuestras partes interesadas, mediante la prestación de servicios que cumplan estos requisitos a través de los sistemas de gestión implantados.

La presente Política se define para establecer un marco de gobierno y control en la organización acorde a los estándares reconocidos basándose en el establecimiento de objetivos de calidad, seguridad de la información y medioambiente.

La Dirección de Grupo Mnemo muestra su compromiso para el correcto desempeño del sistema de gestión, estableciendo las siguientes directrices:

- Asegurar el cumplimiento de los requisitos legales, normativos, contractuales que sean de aplicación, así como otros requisitos que la organización considere oportuno asumir voluntariamente, para mantener un sistema de gestión que le permita conseguir una mejora continua.
- Demostrar una sólida responsabilidad con el entorno que nos rodea, siendo uno de nuestros principales compromisos la prevención de la contaminación, protección ambiental, y la mitigación de los aspectos ambientales derivados de la actividad de Mnemo, y otros compromisos específicos pertinentes al contexto de la organización.
- Dar cumplimiento a las necesidades y expectativas de las partes interesadas involucradas en los sistemas de gestión.
- Dotar de las medidas técnicas y organizativas necesarias para garantizar la Seguridad de la Información de Grupo Mnemo y las partes interesadas involucradas.
- Concienciar a todo el personal del cumplimiento de esta Política y los procesos definidos, así como el desempeño de sus funciones relacionadas con la calidad, seguridad de la información y medioambiente.
- Asignación de los roles necesarios, junto con sus funciones y responsabilidades para el correcto desarrollo del Sistema de Gestión y el desempeño de los procesos de la organización.
- Proveer por parte de la dirección de Grupo Mnemo los recursos necesarios para su plena implantación y mejora continua de los sistemas de gestión.

- Compromiso en la evolución y mejora continua de los Sistemas de gestión a través:
    - Seguimiento y medición de nuestros procesos internos.
    - Proponer objetivos compatibles con la dirección estratégica de la organización, asegurando el cumplimiento de estos a través de su seguimiento y medición.
    - Gestión de riesgos orientado a los procesos y activos de la organización.
    - Seguimiento y medición del grado de satisfacción de nuestros clientes.
    - Revisiones continuas del sistema de gestión.
    - Establecimiento de indicadores para evaluar la eficacia y eficiencia.
    - Auditorías periódicas y resolución de los hallazgos.

Esta Política de Calidad, Seguridad y Medioambiente, estará vigente desde la fecha de su aprobación por la Dirección de Mnemo y anula a cualquier versión anterior, siendo revisada anualmente.

Raúl Sánchez Alonso
Director General de Grupo Mnemo
Vers.1.0. Fecha Versión: 10/06/2021

2. Política de Seguridad (ENS)

MNEMO EVOLUTION & INTEGRATION SERVICES, S.A. (en adelante Mnemo), es una empresa española cuya misión es prestar servicios de Tecnología y Seguridad de alto valor añadido y máxima calidad, siendo percibidos por nuestros clientes como una opción de seguridad y confianza en los productos y servicios que ofrecemos.

Para alcanzar estos objetivos, Mnemo depende de los sistemas TIC (Tecnologías de Información y Comunicaciones). Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad o privacidad de la información tratada o los servicios prestados. El objetivo de la seguridad es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Consciente de esta importancia de las TIC, Mnemo ha implantado un sistema de gestión de la información basado en el Esquema Nacional de Seguridad (ENS) y la legislación aplicable en Protección de Datos Personales.

En este contexto, se han establecido los siguientes **principios rectores** que deben guiar permanentemente nuestra actuación en este ámbito:

- Comprensión y satisfacción de las expectativas de las partes interesadas (clientes, empleados, socios tecnológicos, colaboradores…) en todo lo referente a la seguridad.
- Establecimiento de objetivos, enfocados hacia la evaluación del desempeño en materia de seguridad, así como a la mejora continua de las actividades y del Sistema de Gestión que desarrolla esta política.
- Aseguramiento de que el modelo de gestión de la seguridad persiga una adaptación permanente a los cambios en las condiciones del entorno para prevenir, detectar, reaccionar y recuperarse de incidentes y garantizar la prestación continua de los servicios. En esta línea, los departamentos deberán:
  - Aplicar las medidas mínimas de seguridad exigidas por la normativa en vigor y las derivadas de las evaluaciones periódicas de amenazas y riesgos,
  - Realizar un seguimiento continuo de los niveles de prestación de servicios, así como realizar el análisis y seguimiento de las vulnerabilidades reportadas.
  - Asegurar que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.
  - Definir los requisitos de seguridad y las necesidades de financiación que deberán ser incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

- Definir y documentar de forma clara estas medidas y los roles y responsabilidades de seguridad del personal involucrado.
- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Establecer mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros preestablecidos como normales.
- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones bidireccionales con Equipos de Respuesta a Emergencias (CERT).
- Desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación que garantizar la disponibilidad de los servicios críticos.
- Proteger la seguridad y salud de sus trabajadores, así como el desarrollo de un adecuado ambiente de trabajo.

- Igualmente, y dada su relevancia, todos los empleados y colaboradores de Mnemo deberán mantener un fuerte compromiso con la seguridad. En este sentido deberán:
  - Conocer y cumplir esta Política de Seguridad y la normativa de seguridad aplicable.
  - En línea con lo anterior, cumplir íntegramente con las pautas establecidas de gestión de la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad y privacidad de la información, tanto las generales como las que puedan aplicar a grupos específicos, incluyendo:
    - ✓ Control de accesos,
    - ✓ Seguridad física en las instalaciones.
    - ✓ Formación, concienciación y motivación en seguridad.
    - ✓ Conocimiento de roles y responsabilidades.
    - ✓ Gestión de la continuidad del negocio.
    - ✓ Consecuencias de la falta de cumplimiento de las políticas de seguridad.

  - ✓ Apoyo en la gestión de la seguridad.
  - ✓ Cumplimiento con la legislación.
  - ✓ Buenas Prácticas del usuario.
- Mostrar la máxima diligencia en la comunicación de posibles incidentes de seguridad a través de los canales establecidos para ello.
- Apoyar a la estructura organizativa establecida para cumplir los objetivos de control de la seguridad y gestión continua de los riesgos.
- Utilizar correctamente las instalaciones y el equipamiento asignado, de forma tal que este uso esté en correspondencia con la actividad y objetivos de la organización establecidos.
- Asistir a las sesiones de formación y concienciación sobre gestión de la seguridad a las que sean convocados. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de dichos sistemas en la medida en que la necesiten para realizar su trabajo.

MARCO NORMATIVO

El marco legal y regulatorio en el que se desarrollan nuestras actividades viene determinado por:

- Ley 31/1995, de 8 de noviembre de prevención de riesgos laborales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y Comercio Electrónico.
- Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.
- Real Decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Resolución de 22 de febrero de 2018, de la Dirección General de Empleo, por la que se registra y publica el XVII Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

garantía de los derechos digitales.

- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

DESARROLLO DE LA POLÍTICA DE LA SEGURIDAD

De esta manera la Política de Seguridad se desarrollará por medio de una normativa de seguridad (procedimientos, instrucciones de trabajo y formatos) que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

En concreto, nuestro sistema de gestión desarrolla esta Política de Seguridad de forma ordenada y fácil de comprender, quedando estructurado según el siguiente modelo:

POLÍTICA
PROCEDIMIENTOS
INSTRUCCIONES DE TRABAJO
FORMATOS
Registros

Este desarrollo del SG queda encomendado al Responsable del Sistema de Gestión. El sistema estará disponible en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos de acuerdo con nuestro procedimiento en vigor de gestión de los accesos. En todo caso, el criterio general a considerar es que cada colaborador debe tener acceso siempre a la Política de Seguridad y a toda la normativa que pueda ser relevante para el correcto desempeño de su trabajo.

DATOS DE CARÁCTER PERSONAL

Mnemo trata datos de carácter personal (empleados, candidatos y, eventualmente de clientes…). A estos datos sólo tendrán acceso las personas autorizadas, identificándose y analizándose los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa según la naturaleza y finalidad de los datos de carácter personal recogidos y tratados.

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 periódicamente (al menos una vez al año) y cuando:

- Cambie substancialmente la información gestionada.
- Cambien substancialmente los servicios prestados.
- Ocurra un incidente grave de seguridad.
- Se reporten vulnerabilidades graves.

La gestión de riesgos se realizará según metodologías y procedimientos reconocidos en el mercado, quedando documentada la mecánica de identificación, valoración y tratamiento de riesgos.

TERCERAS PARTES

Cuando Mnemo preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad, se establecerán canales para reporte y coordinación con los responsables de los servicios involucrados y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Mnemo utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Para ambas situaciones, se definirán procedimientos específicos de reporte y resolución de incidencias relacionadas con la seguridad.

ORGANIZACIÓN DE LA SEGURIDAD

La gestión de nuestro Sistema de Gestión se encomienda al Responsable del Sistema de Gestión. Los roles o funciones relacionados con la seguridad son:

Función	Deberes y responsabilidades
Responsable de la información	Tomar las decisiones relativas a la información tratada
Responsable de los servicios	Coordinar la implantación del sistema Mejorar el sistema de forma continua
Responsable de la seguridad	Determinar la idoneidad de las medidas técnicas

	Proporcionar la mejor tecnología para el servicio
Responsable del sistema de gestión	Coordinar e impulsar la implantación del sistema de gestión Mejorar el sistema de gestión de forma continua
Responsable de los sistemas TIC	Coordinar e impulsar la implantación de los sistemas TIC Mejorar los sistemas TIC de forma continua
Dirección	Proporcionar los recursos necesarios para el sistema Liderar el sistema

Esta definición se completa en los perfiles de puesto y en los documentos del sistema. El procedimiento para su designación y renovación es la ratificación en el Comité de Calidad, Seguridad y Medioambiente, órgano ejecutivo y con autonomía para la toma de decisiones y que no subordina su actividad a ningún otro elemento de nuestra empresa.

Este Comité es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad, tomando todas las decisiones relevantes relacionadas con la misma. Sus decisiones quedan reflejadas en las actas.

3. Política de la Gestión de Servicios (SGS)

MNEMO EVOLUTION & INTEGRATION SERVICES, SA. (en adelante Mnemo), es una empresa española del ámbito de las Tecnologías de la Información cuya actividad fundamental es el desarrollo de grandes proyectos de Tecnología y de Seguridad de la Información.

Siendo consciente de la importancia que para la competitividad de nuestra organización tiene la adecuada prestación de sus servicios, la Dirección ha implantado un Sistema de Gestión del Servicio (SGS) basado en procesos y alineado con los requerimientos de la ISO 20000-1, y ha establecido los siguientes **principios rectores** que deben guiar permanentemente el diseño, transición, provisión y mejora continua de nuestros servicios:

- Asegurar el entendimiento y cumplimiento de los requisitos de servicio para lograr la satisfacción del cliente y de cualquier otra parte interesada.
- Monitorizar, medir y revisar el comportamiento del SGS y de los servicios identificados en el portafolio.
- Analizar de forma continua todos los procesos internos relevantes relacionados con la prestación de servicios, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Definir periódicamente objetivos enfocados en la mejora continua de las actividades y del Sistema de Gestión que desarrolla esta política, revisando su grado de implantación.
- Cumplir los requisitos legales aplicables y otros requisitos, incluyendo los compromisos adquiridos con los clientes, proveedores y socios, y toda aquella reglamentación, normas internas o pautas de actuación a los que voluntariamente se someta la empresa.
- Asegurar la implicación y seguimiento por parte de la Dirección en la Gestión de los Servicios.
- Integrar los objetivos de la Gestión de los Servicios con la misión y objetivos de Mnemo y de las partes interesadas.
- Informar a todos los empleados de sus funciones, obligaciones y responsabilidades en lo que respecta a la gestión del servicio.
- Formar y concienciar al personal en materia de gestión de los servicios.
- Definir y poner en marcha los roles y responsabilidades dentro de la organización, que se encarguen de gestionar el sistema y velar por el desarrollo, mantenimiento y mejora del mismo.

La presente política es conocida y suscrita por todo el personal de Mnemo contemplado en el alcance, conforme a las exigencias de la dirección.

Esta política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la dirección de la organización.

Raúl Sánchez Alonso
Director General de MNEMO Evolution & Integration Services, S.A.
Vers.2.2. Fecha Versión: 12/11/2020

4. Política de Continuidad de Negocio (SGCN)

MNEMO EVOLUTION & INTEGRATION SERVICES, SA. (en adelante Mnemo), es una empresa española del ámbito de las Tecnologías de la Información cuya actividad fundamental es el desarrollo de grandes proyectos de Tecnología y de Seguridad de la Información.

Siendo consciente de la importancia que para su competitividad empresarial tiene la adecuada gestión de la continuidad de sus actividades, la Dirección ha implantado un Sistema de Gestión de la Continuidad del Negocio alineado con los requerimientos de la ISO 22301, y ha establecido los siguientes **principios rectores** que deben guiar permanentemente nuestra actuación en este ámbito:

- Comprensión y satisfacción de las expectativas de las partes interesadas en todo lo referente a la continuidad de nuestra actividad. Estas expectativas deberán ser expresadas en términos acordes con prácticas reconocidas en este campo.
- Establecimiento de objetivos de continuidad que puedan ser adecuadamente evaluados y que sirvan de base para la mejora continua de las actividades y del Sistema de Gestión que desarrolla esta política, revisando su grado de implantación.
- Cumplimiento de los requisitos legales aplicables y otros requisitos, incluyendo los compromisos adquiridos con los clientes, proveedores y socios, y toda aquella reglamentación, normas internas o pautas de actuación a los que voluntariamente se someta la empresa.
- Uso de una metodología adecuada para la gestión de la continuidad, contemplando la realidad de un entorno muy cambiante. En esta línea, la metodología deberá contemplar los siguientes principios:
  - Identificación de las amenazas potenciales, así como el impacto en las operaciones de Mnemo que dichas amenazas, en caso de materializarse, puedan causar.
  - Basado en lo anterior, realización de análisis de riesgos, evaluándose los impactos y objetivos de negocio para la definición de los niveles de recuperación de estos, priorizándose la continuidad de las actividades críticas.
  - Diseño de planes de continuidad para asegurar la recuperación rápida y eficiente de las operaciones esenciales de Mnemo frente a cualquier desastre físico o incidente que ponga en riesgo la continuidad de las operaciones.
  - Revisión y prueba periódica de los planes de continuidad, siendo auditados regularmente con el fin de asegurar su permanente operatividad.
  - Mantenimiento como fin principal del esfuerzo de Mejora Continua el aumento de la capacidad de resiliencia de Mnemo.

- Aseguramiento del correcto estado de las instalaciones y el equipamiento adecuado de forma tal que estén en correspondencia con la actividad, y objetivos de la organización.
- Compromiso de proteger la seguridad y salud de sus trabajadores, así como de desarrollar un adecuado ambiente de trabajo.

El SGCN ha sido elaborado siguiendo las instrucciones y bajo la supervisión de la Dirección General de Mnemo. Se ha diseñado para garantizar la seguridad del personal y de cualquier otra persona que se encuentre en sus instalaciones y para facilitar la vuelta a la operativa normal en el tiempo más breve posible y con la mínima interrupción.

La Dirección General apoya totalmente el SGCN y espera que todo el personal conozca su contenido y que los planes estén listos para ser activados en cualquier momento.

Raúl Sánchez Alonso
Director General de MNEMO Evolution & Integration Services, S.A.
Vers.2.3. Fecha Versión: 12/11/2020