

MNEMO

Políticas de Sistemas de Gestión

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 implantación de	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
04/11/2022	Modificación de la Política de Seguridad ENS	Cumplimiento Normativo	v.1.4
02/03/2023	Se corrige errata en Política de Calidad, Medioambiente y Seguridad Se revisa y adecua la política de seguridad ENS para adaptarla a la nueva norma	Cumplimiento Normativo	v.1.5

10/04/2024	Cambio nombre de documento y adecuación a requisitos de ISO 27001:2023	Cumplimiento Normativo	v.1.6
14/08/2024	Actualización de la política de seguridad ENS tras hallazgos en revisión documental	Cumplimiento Normativo	v.1.7
03/03/2025	Actualización de la política ENS incluyendo otra legislación aplicable	Cumplimiento Normativo	v.1.8

Índice

1. Política de Calidad, Medioambiente y Seguridad de la Información	6
2. Política de Seguridad (ENS)	8
3. Política de la Gestión de Servicios (SGS)	19
4. Política de Continuidad de Negocio (SGCN)	20

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 27001:2023** 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.

2. Política de Seguridad (ENS)

OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN

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 objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos de seguridad y continuidad, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

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, y en cumplimiento con lo establecido en el Artículo 12 del RD 311/2022, esta política de seguridad de la información es el conjunto de directrices que rigen la forma en que Mnemo gestiona y protege la información que trata y los servicios que prestase, de acuerdo con los siguientes principios básicos que se rigen por el Artículo 5 del RD 311/2022 que deben guiar permanentemente nuestra actuación en este ámbito:

- **Seguridad como proceso integral:** constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Prestándose la máxima atención a la concienciación de las personas que intervienen en el proceso para evitar que constituyan fuentes de riesgo para la seguridad.
- **Gestión de la seguridad basada en los riesgos:** esta actividad debe ser continua y permanentemente actualizada. Permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad atendiendo al principio de proporcionalidad.
- **Prevención, detección, respuesta y conservación:** el objetivo es minimizar sus vulnerabilidades del sistema y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.
 - Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a

materializarse.

- Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.
- Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.
- Se debe garantizar la conservación de los datos e información en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.
- **Existencia de líneas de defensa:** El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad (organizativa, física y lógica), dispuesta de forma que, cuando una de las capas sea comprometida, permita:
 - Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
 - Minimizar el impacto final sobre el mismo.
- **Vigilancia continua:** permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. Permite medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
- **Reevaluación periódica:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.
- **Diferenciación de responsabilidades:** En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

La política de seguridad se establecerá de acuerdo con los principios básicos señalados y se desarrollará aplicando los siguientes requisitos mínimos:

- **Organización e implantación del proceso de seguridad:** Cumpliendo con lo establecido en el Artículo 13 del RD 311/2022 Los roles o funciones relacionados con la seguridad son:

Función	Deberes y responsabilidades
Responsable de la información	Determinará los requisitos de la información tratada
Responsable de los servicios	Determinará los requisitos de los servicios prestados
Responsable de la seguridad	Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
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	Desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
Dirección	Proporcionar los recursos necesarios para el sistema Liderar el sistema

Aplicando el principio de diferenciación de responsabilidades recogido en el Artículo 11 del RD 311/2022 el responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos.

En caso de conflicto, este deberá ser elevado al comité de seguridad, siendo resuelto en última instancia la Dirección General, siempre que no haya acuerdo, y será quien decidirá aplicando los principios más restrictivos en materia de seguridad de la información.

No cabe esperar que se produzcan conflictos entre las obligaciones del responsable de la Seguridad derivadas de una u otra normativa, pues siempre deberá cumplirse la mayor de las exigencias derivadas de uno u otro.

No cabe esperar que se produzcan conflictos entre los responsables de la información, y de los servicios, por una parte, y los responsables del fichero y del tratamiento por otra. En caso de discrepancia, los datos de carácter personal constituyen un objeto protegido de mayor rango y marcarán la pauta a seguir.

LA ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ

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 Cumplimiento Normativo, 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. Deberá resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir, a la Dirección General que decidirá en última instancia.

Los servicios externalizados deberán designar un POC con Mnemo para la comunicación de incidentes de seguridad.

- **Análisis y gestión de los 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.

- **Gestión de personal:** 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.
- **Profesionalidad:** Se contará siempre con personal cualificado e instruido para la gestión de la seguridad de los sistemas en todo su ciclo de vida. El personal recibirá la formación que sea necesaria para el correcto desempeño de la seguridad de los sistemas.
 - **Autorización y control de los accesos:** Asegurarse de que el acceso al sistema de información es controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
 - **Protección de las instalaciones:** 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, estableciendo controles para ello.
 - **Adquisición de productos:** Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema, atendiendo siempre a los criterios de seguridad de forma proporcionada a la categoría del sistema y nivel de seguridad determinados
 - **Mínimo privilegio:** Los sistemas son diseñados y configurados de forma que garanticen la seguridad por defecto cumpliendo el principio de mínimo privilegio:
 - El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
 - Las funciones de operación, administración y registro de actividad serán

las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean 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.
- **Integridad y actualización del sistema:** Asegurarse en todo momento de que el estado de seguridad de los sistemas es el apropiado, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.
 - **Protección de la información almacenada y en tránsito:** La información puede ser almacenada en la estructura y organización de seguridad del sistema, que se aplicará por defecto, y en caso de no almacenarse ahí, por cualquier excepción, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, soportes de información, papel, ...
 - **Prevención ante otros sistemas de información interconectados:** El sistema ha de proteger el perímetro.
 - **Registro de actividad y detección de código dañino:** Aseguramiento de que toda la actividad de usuarios quede reflejada en los sistemas de información, y establecimiento de controles que permitan detectar código dañino que afecte a la seguridad de la información.
 - **Incidentes de seguridad:** 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).
 - Proteger la seguridad y salud de sus trabajadores, así como el desarrollo de un adecuado ambiente de trabajo.
- **Continuidad de la actividad:** Desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación que garantizan la disponibilidad de los servicios críticos.
 - **Mejora continua del proceso de 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.

MARCO NORMATIVO

El marco legal y regulatorio en el que se desarrollan nuestras actividades se establece en PG-04.02 Requisitos legales y otros requisitos, particularmente atendiendo al ámbito del ENS son de aplicación

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de

Seguridad de Informe del Estado de la Seguridad

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) N° 910/2014 Radel Parlamento Europeo y del Consejo, de 23 de julio de 2014), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley

37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 14/2023, de 20 de diciembre, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid
- MSI-01 Manual de Políticas de Seguridad de la información en Mnemo

También se consideran las restantes normas aplicables a los servicios bajo el objeto de aplicación del ENS, y comprendidos dentro del ámbito de aplicación de la presente política.

El mantenimiento del marco normativo se llevará a cabo conforme a lo descrito en PG-04.02 Requisitos legales y otros requisitos.

Así mismo, se identificarán las guías de seguridad del CCN, conforme lo descrito en PG-07.05 Información documentada, referenciadas en el mencionado artículo, que se aplicarán en el cumplimiento de lo establecido en el ENS.

DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO

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.

En aquellos casos en los que se cuenta con un encargado de tratamiento, se establecen los acuerdos y condiciones que rigen la forma en la que deben ser tratados acorde a los riesgos detectados por el responsable de protección de datos, que evalúa el tratamiento que debe aplicarse en cada caso, y al que puede acceder para ejercer los derechos contemplados en la legislación a través de la dirección de correo electrónico dpo@mnemo.com

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 atañe 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. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida Mnemo como destinataria de dichos servicios.

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

NIVEL DE SEGURIDAD REQUERIDO

Mnemo ha identificado tres niveles de calificación para la información gestionada por los sistemas de información en los distintos alcances, Bajo, Medio y Alto, para determinarlo, se ha modulado el equilibrio entre la importancia de la información que se maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad. Se valora el impacto que tendrá un incidente que afectará a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad atendiendo a su repercusión en la capacidad de Mnemo para 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 ciudadanos. Los criterios que determinan la categoría del sistema, y por tanto el nivel de seguridad requerido, vienen definidos en el documento *Categorización del Sistema*.

Raúl Sánchez Alonso

Director General de MNEMO Evolution & Integration Services, S.A.

Vers.9.2 Fecha Versión: 03/03/2025

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.