
# Responsabilidades sobre la Seguridad de la Información

## Consideraciones de seguridad



## Información del documento

| | | | |
|---|---|---|---|
| **Documento** | MSI-02 Responsabilidades sobre la Seguridad de la Información | | |
| **Autor/es** | Área de Calidad | | |
| **Revisado por** | Comité de Calidad, Seguridad y Ambiental | | |
| **Aprobado por** | Comité de Calidad, Seguridad y Ambiental | | |
| **Fecha aprobación** | 06/08/2020 | **Fecha de implantación** | 06/08/2020 |

## Historial de cambios

| Fecha | Descripción | Realizado por | Versión |
|---|---|---|---|
| **06/08/2020** | Creación del documento | Área de Calidad | 1.0 |
| **07/10/2020** | Corrección de errata sobre el correo de notificación de incidentes | Área de calidad | 1.1 |
| **18/03/2021** | Se actualizan las definiciones de clasificación de la información | Área de Calidad | 1.2 |
| **27/05/2021** | Se cambia el antiguo correo de servicedesk por la nueva plataforma | Área de Calidad | 1.3 |
| **13/09/2021** | Se cambia el antiguo correo por la nueva plataforma servicedesk.<br>Se revisa el punto de Soportes extraíbles.<br>Se incluyen instrucciones sobre limpieza de documentos (metadatos) | Área CSMA | 1.4 |
| **11/10/2021** | Se indica la necesidad de destruir la documentación en papel en la destructora, previo a su recogida por gestor autorizado. | Área CSMA | 1.5 |
| **05/05/2022** | Se modifican las categorías de clasificación de la información | Cumplimiento Normativo | 1.6 |
| **21/06/2022** | Modificación párrafo de información de carácter personal | Cumplimiento Normativo | 1.7 |

| | | | |
|---|---|---|---|
| **13/04/2023** | Revisión y actualización del documento | Responsable de Seguridad | 1.8 |
| **09/06/2023** | Adecuación de política a requisitos ENS | Responsable de Seguridad | 1.9 |

# Índice

1.- Objetivo ..... 4
2.- Alcance ..... 4
3.- Referencias ..... 4
4.- Definiciones ..... 5
5.- Clasificación de la información ..... 5
6.- Información de carácter personal ..... 6
7.- Responsabilidades sobre la Seguridad de la Información ..... 8
7.1.- Puesto de trabajo y equipo desatendido ..... 8
7.2.- Portátiles y dispositivos móviles ..... 8
7.2.1.- Sobre la protección física ..... 8
7.2.2.- Sobre el uso diario ..... 9
7.2.3.- Sobre el acceso al dispositivo ..... 9
7.2.4.- Sobre el uso de la red wifi ..... 9
7.2.5.- Sobre el uso de Bluetooth ..... 9
7.2.6.- Sobre la protección lógica ..... 9
7.2.7.- En caso de robo o pérdida ..... 10
7.3.- Impresión ..... 10
7.4.- Instalación de software ..... 10
7.5.- Contraseñas ..... 11
7.6.- Correo electrónico ..... 11
7.7.- Internet ..... 12
7.8.- Soportes ..... 13
8.- Gestión de incidentes de seguridad ..... 14
9.- Gestión de incidentes de privacidad ..... 14
10.- Comportamientos negligentes ..... 16

## 1.- Objetivo

El objetivo de este manual es describir las políticas de seguridad y privacidad en **Mnemo** que son de obligatorio cumplimiento por parte de los empleados y/o colaboradores de **Mnemo**, en relación con el uso de los sistemas de información asociados a la operativa de la compañía.

## 2.- Alcance

El alcance de este manual comprende a:

- Todo el personal que tenga una relación laboral con:
  - Mnemo Evolution & Integration Services
  - Mnemo Innovate
  - Mnemo Intelligence
  - Mnemo Colombia
- Todo el personal que tenga una relación mercantil con:
  - Mnemo Evolution & Integration Services
  - Mnemo Innovate
  - Mnemo Intelligence
  - Mnemo Colombia

## 3.- Referencias

Los documentos de referencia para la realización de este procedimiento son:

- Norma Internacional ISO/IEC 27002:2017.
- Política de Seguridad.
- Políticas de seguridad de la Información.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.

## 4.- Definiciones

Consultar el ***https://www.iso.org/obp/ui***

## 5.- Clasificación de la información

En Mnemo la información se clasifica según el siguiente esquema de clasificación basado en la Guía de Seguridad de las TIC CCN ENS Valoración de los sistemas STIC 803:

- **RESERVEDA**: aquella información que debe conocerla un número muy reducido de personas o que trata datos personales sensibles (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, tratamiento de datos genéticos, identificación biométrica, salud, vida u orientación sexual). El impacto se considera máximo:
    - por disposición legal o administrativa
    - porque su revelación causaría un grave daño, de difícil o imposible reparación o porque su revelación supondría el incumplimiento grave de una norma
    - porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
    - porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- **CONFIDENCIAL:** aquella información que deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita o datos de carácter personal. El impacto se considera significativo:
    - por disposición legal o administrativa
    - porque su revelación causaría un daño importante, aunque subsanable
    - porque su revelación supondría el incumplimiento material o formal de una norma o porque su revelación causaría pérdidas económicas importantes
    - porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

- **DIFUSIÓN LIMITADA**: aquella información que no deben conocerla personas ajenas a la organización o sus clientes. El impacto se considera limitado:
    - por disposición legal o administrativa
    - porque su revelación causaría algún perjuicio
    - porque su revelación supondría el incumplimiento leve de una norma o porque su revelación supondría pérdidas económicas apreciables
    - porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
- **DIFUSIÓN PUBLICA:** información de carácter público, accesible por cualquier persona. Su impacto se considera despreciable.

En **Mnemo** toda la información reservada, confidencial o de difusión interna debe encontrarse debidamente etiquetada, indicando en las cabeceras o pies de página la clasificación de la información que contenga el documento.

Para realizar un correcto uso de la información, se debe tener en cuenta que:

- La información reservada y confidencial es responsabilidad de su propietario.
- La información reservada, confidencial o de uso interno sólo se puede transmitir según los fines previstos.
- Cuando algún empleado o colaborador este autorizado para realizar alguna gestión sobre la información de **Mnemo**, éste se hará responsable del buen cuidado de esta información.
- La información reservada o confidencial no se almacenará en los equipos, dispositivos móviles o soportes extraíbles.
- El Responsable de la Información o activo, es el responsable de la destrucción de esta, para ello, seguirá las pautas aprobadas por **Mnemo**. La información reservada o confidencial en formato papel se debe de eliminar solamente en las destructoras habilitadas al efecto.
- Se deberán eliminar todos los metadatos de los ficheros que por causa de la operativa propia del negocio deban ser compartidos con terceras partes.

## 6.- Información de carácter personal

Las obligaciones de todo empleado o colaborador de **Mnemo** deberá cumplir en el tratamiento de datos de carácter personal, en lo relativo a la seguridad de dichos datos, se regirán por las leyes y reglamentos en los países donde opere **Mnemo**.

Se define como dato personal: "*toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de*

*identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*".

Esta política pretende informar a todos los empleados o colaboradores de **Mnemo** de las obligaciones y responsabilidades que debe cumplir al tratar datos de carácter personal, las cuales son:

- Se prohíbe la creación de ficheros que traten datos de carácter personal sin la previa autorización del Responsable de Tratamiento y sin la supervisión del Delegado de protección de datos (DPO) de **Mnemo**.
- No se tratarán ficheros con datos de carácter personal en dispositivo alguno (físico, electrónico, papel) propiedad de los empleados o colaboradores de **Mnemo**. Los ficheros con datos personales sólo se ubicarán en los servidores, Herramientas o Repositorios documentales de **Mnemo**.
- En referencia a los datos personales, el empleado o colaborador de **Mnemo**, estará obligado a guardar secreto sobre los datos de carácter personal y cualquier información o circunstancia relativa a los clientes, usuarios y otras personas cuyos datos conozca y a los que haya tenido acceso en el ejercicio de las funciones que le hubiesen sido asignadas por **Mnemo**.
- No se revelará información de datos personales a la que se hubiera tenido acceso a ninguna persona ajena o interna de **Mnemo**, ni se le facilitará soporte alguno conteniendo datos de carácter personal sin haber obtenido la debida autorización del Responsable del Tratamiento y siempre bajo la supervisión del Delegado de protección de datos (DPO) de **Mnemo**.
- Aquellos empleados o colaboradores de **Mnemo** que desempeñen sus funciones bajo un marco contractual establecido entre **Mnemo** y sus clientes o socios comerciales, deberán seguir además de lo indicado anteriormente, las medidas técnicas y organizativas vigentes en dicho marco.

Las infracciones por incumplimiento de la normativa en referente a la seguridad de los tratamientos realizados en el seno de **Mnemo** pueden suponer importantes sanciones económicas y afectar a la imagen de **Mnemo**. Estas podrán ser causa a los empleados de **Mnemo** de la apertura de un proceso disciplinario o a los colaboradores de **Mnemo** de la revisión de la relación mercantil o contractual y el inicio de las reclamaciones oportunas.

Las anteriores obligaciones se extienden a cualquier fase del tratamiento de los citados datos y subsistirán aún después de concluidas las funciones en el marco de las cuales ha tenido acceso a los datos o concluida su relación laboral o mercantil con **Mnemo**.

# 7.- Responsabilidades sobre la Seguridad de la Información

El presente apartado pretende informar a todos los empleados o colaboradores de **Mnemo** de las obligaciones que debe cumplir en cuanto al cuidado responsable de los equipamientos y sistemas de información puestos a su disposición.

## 7.1.- Puesto de trabajo y equipo desatendido

- Se debe mantener el puesto de trabajo ordenado, despejado y sin papeles encima del escritorio.
- Al acabar la jornada o cuando te ausentes de tu puesto de trabajo, se deben recoger todos aquellos documentos que puedan contener información confidencial para impedir su visualización, robo y/o pérdida. Para ello debe ser guardada en cajoneras o taquillas cerradas con llave.
- Los empleados o colaboradores de **Mnemo** que tengan acceso a información confidencial deberán asegurarse de que dicha información no sea visible por personas no autorizadas. Procurando que la ubicación de los puestos de trabajo e impresoras sea tal que permita garantizar dicha confidencialidad.
- Cuando se aleje de su puesto de trabajo, el usuario debe bloquear el equipo (Windows + L). En todo caso, los equipos deben configurarse para que después de un período de inactividad de cinco minutos se active el bloqueo del sistema, siendo necesaria la introducción de la contraseña para poder acceder de nuevo al entorno de trabajo. Si se tiene alguna duda al respecto, se debe contactar con el Departamento de Sistemas a través de la herramienta Servicedesk en la siguiente url https://servicedesk.mnemo.com.
- Está prohibido comer y beber en los puestos de trabajo. Asimismo, se debe tener especial cuidado con el manejo de cualquier producto que pueda verterse sobre los activos de información.

## 7.2.- Portátiles y dispositivos móviles

### 7.2.1.- Sobre la protección física

- Es responsabilidad de cada empleado o colaborador de **Mnemo** velar por la protección física del equipamiento propiedad de **Mnemo**, especialmente contra los daños físicos y medioambientales.
- Cuando el empleado o colaborador de **Mnemo** lleve su portátil o dispositivo móvil consigo fuera de las instalaciones de **Mnemo**, no lo dejara desatendido en ningún momento, salvo que estén en una lugar seguro o debidamente protegidos para evitar que sea sustraído.

- Siempre se debe trabajar y hacer uso de la información sobre los sistemas de información corporativa al ser el repositorio central de información de **Mnemo**.

### 7.2.2.- Sobre la protección de los datos corporativos almacenados

- Es responsabilidad de cada empleado o colaborador de **Mnemo** velar por la protección de los datos almacenados en el equipamiento propiedad de **Mnemo**, especialmente contra acceso no autorizado, interceptación y revelación de información, entre otros.
- Cuando el empleado o colaborador de **Mnemo** lleve su portátil o dispositivo móvil consigo fuera de las instalaciones de **Mnemo**, no lo dejara desatendido en ningún momento, salvo que estén en un lugar seguro o debidamente protegidos, a salvo de hurtos y miradas indiscretas.
- Siempre se debe trabajar y hacer uso de la información sobre los sistemas de información corporativa al ser el repositorio central de información de **Mnemo**.
- Se debe atender a la clasificación de la información, a la hora de tratar los datos corporativos.

### 7.2.3.- Sobre el uso diario

- No se utilizarán los equipos de **Mnemo** para cualquier finalidad distinta de las estrictamente profesionales.

### 7.2.4.- Sobre el acceso al dispositivo

- Se debe tener activado el acceso mediante contraseña, datos biométricos o PIN para acceder a las funcionalidades de los equipos.

### 7.2.5.- Sobre el uso de la red wifi

- Se debe de mantener desactivada la red Wi-fi mientras no se vaya a utilizar.
- No se deben hacer uso de las redes Wi-fi públicas o de aquellas que no ofrezcan confianza.

### 7.2.6.- Sobre el uso de Bluetooth

- Se debe desactivar el bluetooth mientras no se vaya a utilizar. En caso de que se vaya a utilizar, hay que configurarlo en modo oculto y con necesidad de contraseña, para que no pueda ser descubierto por atacantes.
- No se deben aceptar conexiones entrantes de dispositivos que se desconozcan para evitar transferencias de contenidos no deseados.

### 7.2.7.- Sobre la protección lógica

- Sólo debe utilizarse el antivirus corporativo, que debe estar permanentemente activado y actualizado. En el caso de inactividad, debe comunicarse

inmediatamente con el Departamento de Sistemas a través de la herramienta Servicedesk en la siguiente url https://servicedesk.mnemo.com para su solución.

- El equipo debe tener configurada la actualización automática del sistema operativo, así como la de los paquetes informáticos (software) instalados. En caso de cualquier anomalía deberá comunicarse inmediatamente con el Departamento de Sistemas a través de la herramienta Servicedesk en la siguiente url https://servicedesk.mnemo.com.

### 7.2.8.- En caso de robo o pérdida

- En caso de robo o pérdida de un portátil, cualquier otro dispositivo electrónico o documentación propiedad de **Mnemo**, el empleado o colaborador de **Mnemo** debe actual del siguiente modo:

  1. Denunciar el robo a las autoridades en menos de 24 horas.
  2. Entregar copia de la denuncia y una breve descripción adicional del tipo de información sustraída o perdida a su Responsable de Departamento o Área, y al Responsable de Sistemas en la mayor brevedad posible.
  3. Informar al Departamento de Sistemas a través de la herramienta Servicedesk en la siguiente url https://servicedesk.mnemo.com.

### 7.2.9.- Sobre el uso de dispositivos móviles personales

- Se permitirá la utilización de aplicaciones corporativas en el terminal personal necesarias para el desempeño de las funciones del puesto de trabajo, siempre y cuando no se tenga asignado un terminal corporativo y que no almacenen localmente datos empresariales, a excepción del correo electrónico.

## 7.3.- Impresión

- Por norma general queda prohibida la impresión de documentos que contengan información de carácter personal o confidencial.
- En caso de tener que recurrir al uso de la impresora, se debe asegurar que no queden documentos impresos en la bandeja de salida.
- Para su eliminación los documentos en papel que lleguen al final de su vida útil deben ser pasados previamente por la destructora para su posterior depósito y recogida por un gestor autorizado.

## 7.4.- Instalación de software

- No se permite la instalación de ningún software adicional a los registrados por el Departamento de Sistemas en los equipos propiedad de **Mnemo**, sin la expresa autorización del Departamento de Sistemas. En caso de ser necesario

para un proyecto o contrato específico la instalación de un software específico será necesaria la autorización del Responsable de Departamento o Área.

- Las herramientas del puesto de trabajo solamente deben ser instaladas por parte del personal autorizado del Departamento de Sistemas, salvo que dicho departamento autorice expresamente a que el usuario realice la instalación.
- Previamente a la instalación, se deben leer los acuerdos de usuario o las características del software para prevenir la instalación o uso de componentes no deseados (software espía).
- Solo deben instalarse aplicaciones que provengan de fuentes oficiales y seguras. No se debe descargar software de sitios poco fiables o sospechosos para impedir la entrada por esta vía de códigos potencialmente maliciosos.
- El departamento de Sistemas tiene el derecho de realizar una auditoría del software instalado en cualquier equipo propiedad de **Mnemo** en cualquier momento.
- No se permite la desinstalación o desactivación de funciones de todo aquel software del puesto de trabajo instalado por el Departamento de sistemas, incluyendo software de monitorización, inventario o soporte remoto entre otros.

## 7.5.- Contraseñas

- Todos los accesos a los equipos, dispositivos móviles o herramientas deben encontrarse protegidos mediante contraseñas o pines. Estas deberán tener una combinación de caracteres alfanuméricos mayúsculas, minúsculas y especiales, con una longitud igual o superior a 10 caracteres.
- Cada nombre de usuario y contraseña es personal e intransferible, y no debe ser compartido Siendo responsabilidad del usuario la custodia de las contraseñas o pines con el fin de salvaguardarlas.
- En caso de que la contraseña o pin sea revelada de forma fortuita o fraudulentamente por personas no autorizadas, ésta se debe cambiar lo antes posible, contactando con el Departamento de Sistemas a través de la herramienta Servicedesk en la siguiente url https://servicedesk.mnemo.com. Se debe desconfiar de cualquier mensaje de correo electrónico en el que se soliciten la contraseña o se indique que se debe visitar un sitio Web para comprobarla. Casi con total seguridad se trata de un fraude.

## 7.6.- Correo electrónico

- Se debe de realizar un uso responsable del correo electrónico corporativo, evitando que este afecte negativamente al rendimiento del empleado o

colaborador de **Mnemo** y restringiéndose solo a las actividades relacionadas con el desempeño profesional.

- No se abrirán correos, enlaces o adjuntos sospechosos procedentes de desconocidos o que no se hayan solicitado, ya que inducen a descargas o accesos a sitios potencialmente peligrosos, por lo que deberán ser eliminados o reportados para su análisis a través del a través del envío de un correo electrónico a la dirección cert.intellsoc@mnemo.com. Si requiere asistencia urgente, incluya la palabra **[URGENTE]** en el asunto.
- Se debe evitar en lo posible la apertura de correo basura o spam, que a menudo, incluye malware, y nunca hacer clic en un vínculo de un mensaje que sea spam.
- Los empleados o colaboradores de **Mnemo** son responsables de todas las actividades realizadas con las cuentas de correo y su respectivo buzón de correos proporcionados por **Mnemo,** y deberá destinarlos a un uso estrictamente profesional. Se prohíbe realizar cualquiera de las siguientes actividades:
  - Falsificar cabeceras de correo electrónico.
  - Enviar correos a través de cuentas ajenas sin consentimiento de su titular.
  - Enviar a foros de discusión listas de distribución, newsgroups o mensajes que comprometan la reputación de **Mnemo**.
  - Utilizar la cuenta de correo corporativa para registrarse en las redes sociales como Facebook, Twitter ..., salvo que sea por razones estrictamente profesionales.
  - Facilitar las cuentas de correo a desconocidos.

## 7.7.- Internet

- Los empleados o colaboradores de **Mnemo** son responsables de las sesiones iniciadas de Internet desde sus equipos de trabajo.
- Queda prohibido la utilización de Internet para las necesidades personales, tales como la navegación, redes sociales, servicios de chat, foros, páginas de juegos y similares, streaming, …, siempre y cuando, estas interfieran con la red de comunicación de **Mnemo**.
- Si se utilizan web para las necesidades personales se debe evitar la aceptación de "cookies" de aquellas webs que se hayan utilizado para el uso personal, evitando así la contaminación entre el uso personal y corporativo.
- Se debe evitar el uso de sitos, las redirecciones que pueden llevarte a sitios totalmente diferentes de los que indican los vínculos, el dar clic o marcar cualquier casilla en sitios de Internet que no sean de seguros, esto puede bastar para dar la autorización necesaria para que penetre malware en el equipo.

- Se debe evitar descargar contenido gratis en sitios que no sean de seguros, dado que es el método de preferido para distribuir Spyware y Troyanos al estar incluirlos en el interior de pequeñas aplicaciones gratuitas y populares.
- Se prohíbe expresamente el acceso y/o descarga y/o almacenamiento en cualquier soporte de páginas y contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres, de los formatos de imágenes, sonido y vídeo; de virus y códigos maliciosos y, en general, todo tipo de programas sin la expresa autorización del Responsable de Departamento o Área.
- El Departamento de Sistemas puede realizar las auditorías de acceso a Internet en cualquier momento sin previo aviso.

## 7.8.- Soportes

- Como norma general, en **Mnemo** **no se utilizarán soportes extraíbles** para la información.
- En caso de que sea necesario disponer de algún soporte para cubrir necesidades operativas de **Mnemo**, solamente se utilizarán los soportes proporcionados por el Departamento de Sistemas, previa solicitud y posterior autorización a través del Servicedesk.
- El Departamento de Sistemas, deberá gestionar el uso de los soportes asignados al Departamento o área solicitante a través de:
    1. Un inventario de los soportes utilizado.
    2. Registro de las entradas y salidas.
    3. Aprobación del Responsable del Departamento o área solicitante para su uso, describiendo la información que contendrá y su necesidad de uso.
    4. Cifrarse si contienen información de carácter personal o confidencial.
    5. Eliminar la información después de su uso.
    6. Asegurarse de la destrucción segura del soporte una vez finalice su vida útil.
- El usuario será responsable en todo momento de la custodia y utilización del soporte que se le ha sido cedido para la realización de sus responsabilidades profesionales.
- Los soportes deberán ser siempre vigilados y guardados bajo llave en el caso de no se estén haciendo uso de éstos.

## 8.- Gestión de incidentes de seguridad

Los empleados o colaboradores de **Mnemo,** que se percatan o tienen conocimiento de algún evento o punto débil que pueda afectar a la seguridad de la información en **Mnemo**, como, por ejemplo:

- Comportamientos extraños del equipo asignado por Mnemo.
- Descarga de la batería anormal.
- Esperas anormales para abrir aplicaciones.
- Llamadas o mensajes no requeridos.
- Posible virus o comportamiento anormal de algún sistema.
- Sistemas o recursos no disponibles.
- Detección de accesos no permitidos a determinada información.
- Robo de información o de cualquier otro activo.
- Abuso o uso no adecuado de recursos como: ordenadores, portátiles, agendas, etc.
- Abuso o uso no adecuado de recursos como: Internet, correo electrónico, red de área local, etc.
- Pérdida de información o información inexacta o corrupta.
- Información clasificada como confidencial o personal expuesto.

Si se detecta alguna anomalía, el empleado o colaborador de **Mnemo** debe contactar con el Departamento de Sistemas a través de la plataforma Servicedesk en la siguiente url https://servicedesk.mnemo.com.

Al informar sobre este tipo de incidentes de seguridad, los empleados o colaboradores recibirán asistencia técnica para su resolución. Esto también, ayudará a **Mnemo** a correlacionar los incidentes, reportarlos, analizarlos y sacar conclusiones; para difundir la información actualizada y desarrollar pautas de seguridad efectivas para prevenir la ocurrencia de incidentes en el futuro.

Hay que tener en cuenta que el conocimiento y la no notificación de una incidencia por parte de un empleado será considerado como una falta contra la seguridad por parte de ese usuario.

## 9.- Gestión de incidentes de privacidad

Los empleados o colaboradores de **Mnemo**, que se percatan o que tienen conocimiento de algún evento o punto débil que pueda afectar a la información de carácter personal en **Mnemo**, como, por ejemplo:

- Recabar datos de carácter personal sin la autorización del afectado y sin informarle de sus derechos.
- Uso de los datos de carácter personal para otra finalidad diferente a la registrada en el Registro de actividad.
- Violación de los sistemas de control de acceso.
- Borrado fortuito o intencionado de datos de carácter personal.
- Salida de datos en soportes físicos o lógicos (email) sin la autorización pertinente.
- Salida de datos en soportes diferentes a los autorizados en el registro de la base de datos.
- Incumplimiento de los plazos establecidos para resolver y contestar las solicitudes de acceso, rectificación, borrado y oposiciones recibidas de los afectados.
- Uso ilícito de datos de carácter personal.

Si se detecta algún incidente de privacidad o anomalía, el empleado o colaborador de **Mnemo** debe de notificárselo en menos de **24 horas** al DPO a través del envió de un correo electrónico a dpo@mnemo.com quien comunicará a sistemas para la gestión de este incidente.

Hay que tener en cuenta que el conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad por parte de ese usuario.

## 10.- Comportamientos negligentes

**Mnemo** es una empresa de tecnológica que presta a sus clientes servicios de alto valor añadido en el ámbito de la ciberseguridad y de las tecnologías de la información. Nuestros clientes esperan y confían en que nuestra operativa se ajuste a los más altos estándares de exigencia técnico-profesional. Por esta razón, **Mnemo** ha elaborado este manual que recopila y describe aquellas prácticas de trabajo que el mercado, y las diferentes normativas técnicas que se consideran de referencia, consideran de obligado cumplimiento para la ejecución diligente y profesional de actividades del tipo de las que son desarrolladas por nuestra compañía. Por esta razón, el incumplimiento injustificado de estas pautas debe ser considerado como un comportamiento no aceptable y negligente que, como tal, puede ser objeto de sanción.

El incumplimiento, por parte de los empleados de **Mnemo,** de las obligaciones descritas en este documento de forma que cause una brecha de seguridad en la compañía, supondrá la investigación inmediata de dicha violación de seguridad y, en su caso, la apertura de un proceso disciplinario en línea con lo establecido en el ***Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública*** o, en su defecto, en el ***Estatuto de los trabajadores.***

Igualmente, y dada la importancia de los temas descritos, cualquier empleado que tenga conocimiento de alguna situación en la que no se cumplan los principios de actuación descritos en este documento, deberá informar al Responsable de Seguridad o al DPO lo antes posible. Disponer de esta información y no comunicarla a tiempo y en su debida forma podrá, según las circunstancias, ser sancionado de igual manera que la propia infracción.

En un eventual proceso disciplinario se tendrá en cuenta factores tales como la naturaleza y gravedad del incumplimiento y su impacto final en el negocio, así como cualquier otro factor que, de forma razonable, pueda haberlo condicionado (si es la primera vez que se ocurre o se trata de una infracción repetida, si el causante estaba adecuadamente formado, si informó proactivamente del suceso o lo silenció, etc.).

En las situaciones de mayor gravedad, el incumplimiento de las obligaciones descritas en este documento podrá suponer la revisión total de la relación mercantil o contractual, y la ejecución de reclamaciones de cualquier índole según lo establecido en la legislación vigente.

En todo caso, la finalidad principal de este manual es orientar e impulsar a los empleados o colaboradores de **Mnemo** al mayor cumplimiento posible de dichas prácticas como factor ineludible de competitividad de la compañía, debiéndose poner el foco de atención en la adecuada comunicación y comprensión, por parte de los empleados o colaboradores de **Mnemo**, de los principios expuestos en este documento. Los empleados o colaboradores deberán solicitar todas las aclaraciones que consideren oportunas para una comprensión completa de los principios de actuación descritos.

## 11.- Contactos con las autoridades

En el caso que sea necesario contactar con las autoridades debido a un incidente de seguridad, estos son los principales contactos:

| | Autoridad | Teléfono | Email | Web |
|---|---|---|---|---|
| | MNEMO España | 91 417 67 76 | ciso@mnemo.com / dpo@mnemo.com | https://www.mnemo.com/ |
| | MNEMO Colombia | (+571) 691 3133 | solicitudesasg@mnemo.com / ciso@mnemo.com | https://colombia.mnemo.com/ |
| España | Policía Nacional | 091 | | https://www.policia.es/_es/index.php# |
| España | Guardia Civil | 062 | | https://www.guardiacivil.es/es/index.html |
| España | CCN-CERT | | info@ccn-cert.cni.es | https://www.ccn-cert.cni.es/ |
| España | CNI | 91 372 5000 | | https://www.cni.es/ |
| España | INCIBE | 017 | | https://www.incibe.es/ |
| España | AEPD | 900 293 183 | | https://www.aepd.es/es |
| España | Ministerio del Interior | 915 371 000 | | https://www.interior.gob.es/opencms/es/inicio/ |
| Colombia | Equipo de respuesta a incidentes informáticos (CSIRT-PONAL) | 5159090 / 5159586 | | https://cc-csirt.policia.gov.co/ |
| Colombia | ColCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia | 571 2959897 | | http://www.colcert.gov.co/ |
| Colombia | Centro Cibernético Policial | 5715159727 | caivirtual@policia.gov.co | https://caivirtual.policia.gov.co/ |
| Colombia | CSIRT Gobierno | | csirtgob@mintic.gov.co | |
| Colombia | Comando Conjunto Cibernético | | soc-ccoc@ccoc.mil.co | |
| Colombia | Seguridad Digital DNI Dirección Nacional de Inteligencia | 571432-000 | seguridad.digital@dni.gov.co | |
| Colombia | ColCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia | 2959897 | | http://www.colcert.gov.co/?q=contenido/reportarun-incidente |