MNEMO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

Consideraciones de seguridad

La presente documentación es propiedad de **MNEMO** y tiene carácter de **USO INTERNO**. 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	MS-01 Manual de políticas de seguridad de la información y privacidad		
Autor/es	Calidad		
Revisado por	Responsable de seguridad		
Aprobado por	Comité de Calidad, Seguridad y Ambiental		
Fecha aprobación	14/09/2021	Fecha de implantación	14/09/2021

Historial de cambios

Fecha	Descripción	Realizado por	Versión
14/09/2021	Creación del documento	Calidad	v.1.0
27/04/2022	Actualización de políticas de teletrabajo	Calidad	v.1.1
13/04/2023	Actualización de política uso de dispositivos móviles	Responsable de seguridad	v.1.2
09/06/2023	Adecuación a requisitos ENS	Responsable de seguridad	v.1.3

Índice

1.- Objetivo

El objetivo de esta política es establecer un marco de trabajo en Mnemo que permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección tanto de la información como de los sistemas informáticos que gestionan.

2.- Alcance

Este documento aplica a los Sistemas de Gestión implantados en **MNEMO**.

3.- Definiciones

Consultar https://www.iso.org/obp

4.- Responsabilidades

Las responsabilidades del presente procedimiento quedan definidas en la descripción de cada apartado.

5.- Desarrollo

MNEMO EVOLUTION & INTEGRATION SERVICES, SA., MNEMO INNOVATION y MNEMO INTELLIGENCE (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 creciente del trabajo a distancia en el contexto operativo de las organizaciones, Mnemo asume la necesidad de definir unas pautas mínimas que aseguren una operación segura cuando se acude a esta modalidad de trabajo.

La alta dirección de Mnemo ha establecido las presentes Políticas de Seguridad de la Información de acuerdo con las normas ISO/IEC 27001:2013, ISO/IEC 27002:2017, Esquema Nacional de Seguridad (ENS), así como GDPR y LOPDGDD. Dichas normativas establecen el marco tecnológico, organizacional y procedimental para desarrollar, implantar, controlar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI).

El responsable del SGSI ha definido y revisado el presente manual de políticas, con la aprobación del responsable de Seguridad y Delgado de Protección de datos. Dicho responsable se encarga de la coordinación del establecimiento, implantación, revisión y mantenimiento (mejora continua) del SGSI, mediante la aprobación y aceptación de acciones y sus resultados.

El Responsable del SGSI facilita la implantación de las políticas a través de manuales y procedimientos establecidos.

Todo el personal de Mnemo y terceras partes, deberán asumir y cumplir con las normativas de seguridad establecida. Deberán mantener la confidencialidad de la información que tiene acceso debido a su puesto de trabajo. Por otra parte, tienen la obligación de comunicar inmediatamente y de acuerdo con el procedimiento establecido, los incidentes y debilidades de seguridad detectados.

Estas políticas se encuentran disponibles a todas las partes interesadas a través de los canales establecidos en ***FG-07.04.01 Comunicaciones***.

Es necesario que, de forma periódica, al menos anualmente, se revise el contenido de estas políticas para verificar su validez y adaptarlas a las necesidades cambiantes de la operativa de Mnemo

A continuación, se describen los principios donde se sostienen las Políticas de Seguridad y privacidad de Mnemo. Este conjunto de principios fundamentales ha sido formulado basándose en necesidades válidas de negocio, reconocimiento del valor añadido de los sistemas a proteger y una compresión de los riesgos asociados a estos sistemas.

5.1.- Política de Seguridad de la Información y Privacidad a alto nivel

Objetivo:

El objetivo de esta Política es proporcionar las pautas de referencia para el desarrollo de las políticas específicas.

Contenido:

- Se establecerá una política que sea adecuada al propósito de la organización.
- La política deberá incluir objetivos de seguridad de la información y privacidad, o proporcionar un marco de referencia para el establecimiento de los objetivos de seguridad de la información y privacidad.
- Deberá incluir el compromiso de cumplir con los requisitos aplicables a la seguridad de la información y a la protección de la información personal.
- Deberá incluir el compromiso de mejora continua del sistema de gestión de seguridad de la información y privacidad.
- Dicha política deberá estar disponible como información documentada, comunicarse dentro de la organización y estar disponible para las partes interesadas, según sea apropiado.

5.2.- Política de Seguridad de dispositivos móviles

Objetivo:

El objetivo de la presente Política es mantener un nivel de protección de la información contenida en los dispositivos móviles a través de las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de estos dispositivos móviles.

Contenido:

- Se contará con un registro global de todos los dispositivos móviles de la organización, controlando en todo momento los dispositivos autorizados, y a quién están asignados.

- Se deberá concienciar a los usuarios sobre la seguridad física de dispositivos móviles, minimizando así los riesgos de pérdida o robo. Esto se realizará mediante acciones de sensibilización y sobre esta línea, los empleados y colaboradores que utilicen dispositivos móviles deberán seguir las obligaciones y las recomendaciones generales establecidas en el documento ***MSI-02 Responsabilidades sobre la Seguridad de la Información***.

- Los dispositivos móviles que gestionen información confidencial deberán estar sujetos a las medidas de seguridad apropiadas para proteger la información contra software malicioso y que garanticen la no integridad de esta en caso de pérdida o robo de algún dispositivo.

- Siempre que sea posible, aquellos dispositivos móviles que almacenen información personal sensible y que pongan en riesgo los derechos y libertades de las personas deberán estar cifrados).

- Se deberá concienciar a los usuarios sobre los datos corporativos contenidos en los dispositivos móviles, minimizando así los riesgos seguridad de la información. Esto se realizará mediante acciones de sensibilización y sobre esta línea, los empleados y colaboradores que utilicen dispositivos móviles deberán seguir las obligaciones y las recomendaciones generales establecidas en el documento ***MSI-02 Responsabilidades sobre la Seguridad de la Información***.

- 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.

5.3.- Política de seguridad en el trabajo fuera de oficina

Objetivo:

Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.

Contenido:

DISPOSICIONES RELATIVAS AL USO DE EQUIPOS Y TECNOLOGÍA PARA LA OPERACIÓN.

Mnemo deberá:

- Llevar un control de las personas por su perfil dentro de la empresa, considerando que por política de **Mnemo** todo el personal está autorizado para teletrabajar.
- Dar acceso solo a las aplicaciones y servicios necesarios para que cada usuario se conecte remotamente a los recursos o servicios que le corresponda dependiendo de su función en **Mnemo**.
- Limitar el acceso a los recursos y servicios de **Mnemo** a los dispositivos propiedad de la empresa configurados con las políticas de seguridad definidas para tal fin, y bloquear los intentos de acceso a dichos recursos y servicios a todos aquellos dispositivos externos que no pertenezcan a la organización.
- Definir e implementar políticas de contraseñas robustas y el doble factor de autenticación siempre que sea posible, y forzando su cambio periódico. Este mecanismo deberá estar vinculado a la gestión de cuentas de usuarios y control de accesos a través de servicios del Directorio Activo o LDAP.
- Configurar los portátiles para que se mantengan actualizados los sistemas operativos actualizados, antivirus, control de actualizaciones, etc.
- Encriptar La información de datos personales que se encuentra en ordenadores portátiles.
- Finalizar la relación laboral con el empleado (en caso de que suceda) de acuerdo con las normas establecidas en los procedimientos definidos para tal fin.

El trabajador deberá:

- Ejecutar las tareas encomendadas utilizando siempre los medios técnicos proporcionados por Mnemo. Solo se utilizarán, licencias y

herramientas indicadas y verificadas por el área de Sistemas de Mnemo o que sigan las indicaciones del cliente en el caso que así se acuerde.

- No utilizar el equipo corporativo asignado para otros fines distintos a los establecidos a las funciones laborales realizadas en Mnemo.
- No utilizar dispositivos personales para el acceso a los recursos o servicios de Mnemo.
- No utilizar tipos de conexiones que queden expresamente prohibidas por Mnemo (por ejemplo, uso de wifis públicas).
- Evitar el acceso no autorizado a los recursos de Mnemo a personas ajenas, familiares, amigos, etc. que pueden tener accesos desde el puesto donde se realiza la actividad de teletrabajo.
- El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

DISPOSICIONES RELATIVAS A LA PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.

El trabajador deberá…

- Custodiar y proteger la utilización de las credenciales del inicio de sesión para que éstas no sean visibles o accesibles por terceras personas no autorizadas.
- Evitar el acceso a documentos de trabajo por parte de terceras personas no autorizadas, tanto durante la jornada de trabajo como a la finalización de esta.
- Cumplir con todas las medidas de prevención y protección de la información determinadas por el Responsable de Seguridad de Mnemo.
- Comunicar, lo antes posible, cualquier incidencia o malfuncionamiento del equipo asignado a través de la plataforma Servicedesk en la URL: https://servicedesk.mnemo.com

DISPOSICIONES RELATIVAS A LA PROPIEDAD INTELECTUAL DEL TRABAJO REALIZADO.

- Los derechos de propiedad industrial e intelectual de las actividades realizadas bajo esta modalidad de trabajo serán de MNEMO, o de

clientes y/o socios comerciales, de la misma forma que si estos trabajos se hubieran realizado desde sus instalaciones.

DISPOSICIONES RELATIVAS AL CONTROL DEL TRABAJO.

- Mnemo podrá monitorizar y auditar de forma continua las actividades del trabajo a distancia, incluida información, sin carácter limitativo, relativa a geoposicionamiento, inicio de sesión, control de presencia o actividad del usuario, para asegurar el cumplimiento de esta política.

5.4.- Política de seguridad de recursos humanos

Objetivo:

El objetivo de esta política es establecer directrices de seguridad de la información, aplicables al proceso de contratación y administración de personal de RRHH, para asegurarse que los empleados y contratistas conocen sus responsabilidades sobre la seguridad de la información y son adecuados para las funciones que se consideran, así como proteger los intereses de la organización durante el cambio o finalización del empleo.

Contenido:

- Mnemo no deberá recontratar empleados, que hayan sido despedidos por motivos graves.
- Mnemo obligará a firmar un acuerdo de confidencialidad y no divulgación a todos sus empleados y terceras partes colaboradoras.
- La Dirección de Mnemo o los Responsables de las Áreas de Negocio, deberán informar a otras áreas interesadas la baja laboral o despido de un empleado, de modo que se evite que esta persona siga teniendo acceso a las oficinas, equipos o dispositivos de la organización.
- Cuando los empleados de Mnemo, que hayan desempeñado funciones o hayan manejado información sensible de la compañía, son despedidos, deberán de ser acompañados fuera de las instalaciones de Mnemo inmediatamente después del aviso de despido.
- Mnemo deberá asegurarse de la recuperación del material y de la información puesta a disposición de los empleados que salgan, para ello se revisarán todos los activos que se han entregado al empleado al entrar en la empresa y se comprobará que se devuelve todo, entre ellos, el ordenador y teléfono móvil.

- Se comprobará a la salida del empleado despedido de la empresa que no se lleva información, ni documentación en ningún tipo de soporte, salvo aquello que sea privada y/o personal.

- Mnemo posee los derechos exclusivos de la propiedad intelectual de los activos desarrollados por sus empleados.

- Mnemo deberá asegurarse de que todos los empleados han leído y comprendido la política de seguridad de la información y privacidad antes de acceder a la misma.

- Mnemo deberá asegurarse de que el personal, posee la formación necesaria relativa a la seguridad de la información y privacidad para acceder a los sistemas de información.

- Mnemo, pondrá a disposición de cada empleado las políticas de seguridad de la información y privacidad con el fin de que se vaya familiarizando con las normas de aplicación.

- Mnemo deberá de informar a todos los empleados, de cualquier modificación hecha en las políticas de seguridad de la información y privacidad.

- A partir de la aceptación de estas políticas, el incumplimiento de estas conllevará que Mnemo pueda sancionar al empleado con medidas disciplinarias.

5.5.- Política de gestión de activos

Objetivo:

El objetivo de esta política es establecer las directrices de seguridad de la información aplicables a la gestión de activos, identificando los activos y las responsabilidades para la protección. Esta política se aplica a los activos propiedad de Mnemo, o bien a aquellos activos que guarden dependencia con el alcance del SGSI.

Contenido:

- Todos los activos asociados con la información o procesado de la información se encuentran recogidos en un inventario que se mantiene actualizado.
- Todos los activos del inventario tienen designado un responsable o propietario, quien es el responsable de la autorización sobre el uso de estos, estableciendo las medidas que consideren oportunas para su protección.
- El uso aceptable de los activos se describe en el documento ***MSI-02 Responsabilidades sobre la Seguridad de la Información.***

5.6.- Política de protección de datos personales

El 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 junto con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y garantía de los derechos digitales, establece una serie de obligaciones que todo empleado o colaborador de Mnemo que trate datos de carácter personal deberá cumplir, en lo relativo a la seguridad de dichos datos. 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*".

Objetivo:

Esta política pretende informar a todos los empleados o colaboradores de Mnemo de las obligaciones y responsabilidades que deberá cumplir al tratar datos de carácter personal.

Contenido:

- 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

5.7.- Política de seguridad de clasificación de la información

Objetivo:

El objetivo de esta política es establecer las directrices de seguridad de la información aplicables a la clasificación de la información. Esta política se aplica exclusivamente a la información propiedad Mnemo, independientemente del formato y soporte en el que se encuentre (impresa, escrita, electrónica, video, voz, etc.).

Contenido:

- Se seguirán las normas establecidas en Mnemo respecto a la clasificación, marcado y tratamiento de la información.
- Se establecerán los criterios y niveles de clasificación de los activos de información, propiedad de Mnemo, de acuerdo con la importancia para la actividad de Mnemo.
- Las medidas de seguridad implantadas tendrán en cuenta los criterios de clasificación y los requisitos de seguridad establecidos para cada criterio.
- Se designan como propietarios de la información a los directores de cada Área de negocio, o a aquellas personas en las que ellos deleguen dicha responsabilidad de manera formal.
- Los propietarios de la información son los responsables de clasificarla según los criterios definidos, así como de definir los distintos accesos a la misma.
- La clasificación asignada a la información deberá de ser revisada por los propietarios periódicamente.

5.8.- Política de seguridad de utilización de medios

Objetivo:

El objetivo de esta política es establecer las directrices de seguridad de la información aplicables a los medios que puedan contener información. Esta política se aplica exclusivamente a medios de almacenamiento de información propiedad de Mnemo, independientemente del tipo de soporte (soportes extraíbles), para evitar la revelación, modificación, y eliminación no autorizada de la información almacenada.

Contenido:

- Como norma general no se utilizarán dispositivos de almacenamiento.
- En caso de que por la necesidad de negocio se requiera su utilización, se deberán:
    - Ser Inventariados y autorizados por los responsables de cada área de gestión de Mnemo y la dirección de sistemas.
    - Se utilizan los procedimientos de etiquetado de información, conforme a la clasificación de la información definida para la Organización.
    - Se utilizarán procedimientos para utilizar los medios que contienen información, de forma que se respeta la clasificación de la información definida en la Organización.
    - Se utilizarán procedimientos para el manipulado, gestión y destrucción de soportes de información.

5.9.- Política de control de accesos

Objetivo:

El objetivo de esta Política es la definición de normas de seguridad para la gestión de accesos lógicos a los Sistemas de Mnemo, y a las redes y los servicios de red, así como para la definición de los requisitos de seguridad necesarios en los procesos de autenticación, autorización y registro de los sistemas, redes o aplicaciones, limitando el acceso a recursos que albergan información, autorizando el acceso, y responsabilizando al usuario de salvaguardar su información de autenticación, y de este modo prevenir accesos no autorizados.

Contenido:

- Mnemo dispone de un procedimiento de Altas/Bajas o modificaciones del personal, de forma que se establecen los accesos a la información según los perfiles definidos y el nivel de sensibilidad correspondiente.
- Deberá existir consistencia entre los permisos de acceso, y las políticas de clasificación de la información de los diferentes sistemas y redes.
- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switches, etc., deberán cambiarse inmediatamente al ponerse en servicio el equipo.
- Los controles de acceso instalados en los sistemas que utilice Mnemo deberán estar revisados y actualizados.
- Todos los miembros del personal deberán tener nombres de usuario únicos y contraseñas confidenciales que permiten el acceso a los sistemas y a las redes de la organización.
- Un nombre de usuario deberá pertenecer a una sola persona. Está prohibido el compartir y el reutilizar los nombres de usuario.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, ordenadores, redes, y otros recursos del sistema.
- Los privilegios de acceso de un empleado deberán de ser revocados tan pronto el empleado deje de trabajar para la organización.
- Los privilegios del acceso son concedidos por el mando superior apropiado.

- Las cuentas de usuario y los permisos otorgados se revisarán anualmente.
- La detección de una brecha de seguridad en cuentas privilegiadas de usuario exige la modificación automática de las contraseñas de dichas cuentas.
- Los identificadores de acceso para el personal externo deberán diferenciarse del formato habitual para la identificación de los empleados contratados por Mnemo.
- Se controlarán las diferentes formas de acceso existentes a las redes corporativas.
- Se controlarán los requisitos de autenticación de usuario para acceder a los distintos servicios de red.
- En caso de que sea necesario existirá un control de acceso al código fuente de programas.

5.10.- Política de controles criptográficos

Objetivo:

El objetivo de esta Política es la definición de los controles criptográficos que se han considerado necesarios en la organización como parte del SGSI.

Contenido:

- La utilización de controles criptográficos se basará en la Gestión del riesgo. El nivel de protección requerido determinará el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido, así como las claves asociadas.
- Se utilizará cifrado para proteger la información en tránsito, a través de las líneas de comunicación, o en reposo cuando esta resida en dispositivos móviles o en medios extraíbles.
- Se implementarán procedimientos para la gestión de claves y certificados electrónicos.
- Se adaptarán estándares para una implementación efectiva en la organización.
- Se controlará y gestionará la emisión y obtención de certificados de clave pública.
- Se realizará un almacenamiento y custodia de claves, incluyendo cómo los usuarios autorizados obtienen el acceso a las claves.
- Se gestionará el cambio y actualización de las claves, incluyendo las reglas que implican el cambio, y cuando se realiza.
- En el caso que sea necesario, se revocaran claves, incluyendo cómo se procederá a la desactivación de las claves.
- Se gestionará la recuperación de claves por pérdida o por que se corrompieron.

5.11.- Política de seguridad física y del entorno

Objetivo:

El objetivo de esta Política es proporcionar pautas a seguir, referentes a la seguridad física, para:

- Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

- Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Contenido:

- Los edificios y dependencias de Mnemo deberán estar protegidos con controles de entrada y salida adecuados, que garanticen el acceso únicamente al personal debidamente autorizado.

- Los controles de acceso deberán ser operativos, tanto en horas de trabajo como cuando las dependencias permanezcan cerradas.

- Deberán existir al menos los siguientes mecanismos:

    - Prevención: control de acceso a los recursos.

    - Detección: cuando un mecanismo de prevención no existe o no ha funcionado de forma correcta, se deberán detectar los accesos no autorizados a la mayor brevedad posible.

- Las estaciones de trabajo y los equipos informáticos estarán situados, de tal forma que permitan la disminución del riesgo de acceso a la información por visitantes o personas ajenas a Mnemo.

- Está prohibido el uso de cámaras y aparatos de grabación de audio o vídeo dentro de las áreas de seguridad sin autorización previa.

- Los planes de evacuación deberán permitir a los empleados, la información y equipos ser evacuados de forma segura. Las evacuaciones se deberán supervisar por el personal especialmente entrenado. Los lugares evacuados deberán ser bloqueados y supervisados.

- Las infraestructuras y equipamientos de los sistemas de producción de la información deberán situarse en locales seguros, y que tengan las condiciones ambientales controladas.

- Las infraestructuras de tratamiento de la información críticas deberán estar equipadas de sistemas para evitar la Interrupción de flujos eléctricos y supresores de subidas de tensión.

- Los elementos de TIC's correspondientes a activos críticos se ubicarán siempre en lugares donde exista un control de acceso para evitar los accesos no autorizados.

- El cableado eléctrico y de red deberá utilizar rutas adecuadas para evitar peligros del entorno y riesgos de daños por accidentes o actos deliberados.

- Todo el cableado y los conectores deberán estar homologados y cumplir con la normativa aplicable.

- Los cables de red deberán protegerse para prevenir manipulaciones o interceptaciones no autorizadas.

- Las recomendaciones de los proveedores referentes al mantenimiento de los equipos que alberga sistemas de información deberán ser respetadas. Las reparaciones y el mantenimiento se deberán realizar por personal cualificado y autorizado.

- Para sacar cualquier activo fuera del edificio donde se ubican las instalaciones de Mnemo, es necesaria una autorización del propietario del activo, indicando que el empleado ha pedido autorización correspondiente y se la han concedido.

- Se entiende que la concesión de un portátil a cualquier empleado de la empresa conlleva de manera intrínseca la autorización para su salida de la empresa, salvo disposición expresa en contrario por parte del Responsable del Área correspondiente, que podrá restringir la salida cuando lo considere oportuno.

- Se deberá sensibilizar, formar y controlar a los usuarios para que apliquen el principio de escritorio limpio y de puesto desatendido.

5.12.- Política de seguridad de externalización

Objetivo:

El objetivo de esta política es establecer directrices de Seguridad de la Información aplicables en los procesos de externalización de servicios, de cara al tratamiento adecuado de los activos de estos.

Contenido:

- El proveedor, independientemente de su naturaleza, tiene la obligación de adoptar y acreditar la implantación de las Políticas de Seguridad y privacidad de Mnemo, respecto a los activos afectados por el servicio.
- Toda subcontratación de servicios por parte de Mnemo, deberá cumplir al menos, las siguientes directrices de seguridad:
    - Previo inicio del servicio de externalización se deberá proceder a un análisis y evaluación de los riesgos asociados.
    - El acuerdo de nivel de servicio deberá incluir requisitos específicos de seguridad relativos a la confidencialidad, integridad, disponibilidad y privacidad; de acuerdo con la clasificación de la información de los activos del servicio subcontratado.
    - Clara identificación de las obligaciones y responsabilidades legales derivadas de la legislación vigente. Esto incluye la posible aplicación de legislación comunitaria, extracomunitaria o internacional, según la nacionalidad (jurisdicción aplicable) de las partes implicadas en la externalización.
    - Compromiso de confidencialidad respecto a la información a la que el proveedor accede por razón de la externalización.
- Sólo los responsables de la Información (Responsables de Departamento o Servicio) pueden atribuir los privilegios de acceso a la información, aunque existan servicios o tareas externalizadas.
- El contrato con el prestador de servicios deberá estipular que la organización puede recibir una copia completa de la información obtenida y/o elaborada por el prestador del servicio, y que ésta tiene el derecho de exigir dicha información.

5.13.- Política de seguridad para usuarios de los sistemas de información

Esta política está descrita en el ***Manual MS-02 Responsabilidades sobre la Seguridad de la Información.***

5.14.- Política de seguridad de operaciones

Objetivo:

El objetivo de esta Política es establecer operaciones correctas y seguras para todas las ubicaciones de procesamiento de información.

Contenido:

DOCUMENTACIÓN OPERATIVA

- Se deberán documentar y mantener los procedimientos e instrucciones de operación de sistemas.
- La documentación operativa deberá estar accesible a todos los usuarios que la necesiten.

GESTIÓN DEL CAMBIO

- Se identificarán y registrarán los cambios significativos.
- Se procederá a planificar y a verificar los cambios.
- Se valorarán los impactos potenciales, incluyendo impactos de seguridad de la información, debido a cambios.
- Se deberá documentar las aprobaciones formales de los cambios propuestos.
- Se verificará que los requisitos de seguridad de la información son conocidos.
- Se Comunicará todos los detalles del cambio a todas las personas relevantes.
- Se establecerán procedimientos de marcha atrás, incluyendo procedimientos y responsabilidades para abortar, y recuperarse de un cambio no satisfactorio.

GESTIÓN DE LA CAPACIDAD

- Se deberá monitorizar el uso de los recursos, de forma que se puedan hacer proyecciones sobre los requisitos de capacidad futuros, asegurando así el rendimiento requerido del sistema.

SEPARACIÓN DE ENTORNOS DE DESARROLLO, OPERACIÓN Y PRUEBAS

- En aquellos sistemas que así lo requieran se separarán los entornos de desarrollo, pruebas y operación (producción).
- Salvo en circunstancias excepcionales, las pruebas no deberán hacerse en sistemas operacionales.
- La información confidencial o datos personales no deberán copiarse en el entorno de pruebas, a no ser que se implementen controles de seguridad equivalentes a los implantados en el entorno operacional.

PROTECCIÓN CONTRA MALWARE

- Mnemo contará con un sistema de protección frente a cualquier tipo de malware instalado en los sistemas de información.
- Se prohibirá el uso del software no autorizado.
- Se implementarán controles para prevenir la utilización de software no autorizado.
- Se reducirán las vulnerabilidades que pueden ser explotadas con el malware, instalando los parches y actualizaciones publicados por el fabricante.

BACKUP

- Se definirá un plan de copia de Seguridad para disponer de la información en caso de fallo.
- Se deberán acotar y completar los registros de las copias de seguridad, y existirán procedimientos de recuperación.
- Se establecerá la periodicidad, así como el tipo de copia en función de las necesidades del negocio.

LOGS Y MONITORIZACIÓN

- Se habilitarán logs y auditorias en los sistemas implantados en la organización, implicando a identificadores de usuario, actividades del sistema, fechas y tiempos de eventos, cambios en la configuración, direcciones de red y protocolos utilizados.

GESTIÓN TÉCNICA DE VULNERABILIDADES

- Se gestionarán las vulnerabilidades, realizando análisis de vulnerabilidades con una periodicidad mínima anual.

- Los problemas encontrados deberán subsanarse, actualizando el programa afectado y/o instalado un parche en función de la criticidad del problema encontrado.

CONSIDERACIONES PARA AUDITAR SISTEMAS DE INFORMACIÓN

- Los requisitos de auditoría y actividades involucradas en la verificación de los sistemas operacionales deberían de planificarse con cuidado, y con el objetivo de minimizar las interrupciones en la operación de los procesos de negocio.

5.15.- Política de seguridad en las comunicaciones

Objetivo:

Asegurar la protección de la información en redes, y en las instalaciones de procesamiento de información.

Contenido:

GESTIÓN DE LA SEGURIDAD DE RED

- Mnemo deberá asegurar la salvaguarda de la información en las redes y la protección de la infraestructura que la soporta.
- Los servidores de Internet, si existieran, deberán ser protegidos por cortafuegos y estar localizados en una zona desmilitarizada (DMZ).
- Mnemo velará por la seguridad de sus redes frente a posibles ataques tanto internos como externos, utilizando para ello los medios tecnológicos que considere apropiados en cada momento.
- La creación de una conexión directa entre Mnemo y otros ordenadores externos, y viceversa, por medio de una red pública, deberá ser aprobada de antemano, indicando expresamente los protocolos autorizados, empleándose en todos los casos las tecnologías de cifrado que garanticen la confidencialidad de la información por vías inseguras.
- Toda conexión al sistema de Mnemo proveniente del exterior (Internet, líneas telefónicas públicas, etc.), deberá estar protegida por un sistema de control de acceso con una contraseña aprobada.
- Las redes inalámbricas deberán utilizar técnicas de encriptación robustas.
- La organización podrá filtrar las páginas WEB a las que pueden acceder los usuarios con el objetivo de garantizar el uso profesional del servicio.
- Se deberán de verificar de forma periódica los registros (logs) de los sistemas que participan en la red para determinar el correcto estado general del sistema, detectar posibles violaciones o ataques y comprobar la conformidad de éste con las políticas, estándares y procedimientos de seguridad.

- Se deberá verificar cada sistema nuevo que se vaya a instalar en la red antes de pasar al entorno de producción.

- Se intentará proporcionar redundancia de red, tanto en la ruta como en el equipamiento de acceso, para aquellos servicios considerados como críticos.

TRANSFERENCIA DE INFORMACIÓN

- Se diseñan procedimientos para proteger la información transferida de ser interceptada, copiada, modificada o destruida.

- Se implementan controles de protección contra el malware que podría transmitirse a través de las comunicaciones electrónicas.

- Se utilizan técnicas criptográficas para proteger la integridad y confidencialidad de la transferencia.

- Se concienciará al personal para que no revele información confidencial.

- Se tendrán en cuenta los requisitos legales y reglamentarios para la transferencia de información

- Se protegerán los mensajes de correo de accesos no autorizados.

5.16.- Política de seguridad de adquisición, desarrollo y mantenimiento de sistemas de información

Objetivo:

El objetivo de esta Política es definir directrices de seguridad para el proceso de desarrollo de aplicaciones informáticas, bien sea interna o externamente, así como respecto a la adquisición de software comercial. Con ello se busca garantizar la confidencialidad, disponibilidad e integridad de la información soportada por cualquiera de dichas aplicaciones.

Contenido:

- Los requisitos de seguridad deberán garantizar la disponibilidad, confidencialidad e integridad de los activos involucrados.
- Se tendrán en cuenta los requisitos derivados de los procesos de negocio, así como los derivados de los propios controles de seguridad.

SEGURIDAD EN EL DESARROLLO Y PROCESOS DE SOPORTE

- Se contemplará la seguridad desde los entornos del desarrollo, de forma que esté presente desde el comienzo de cada desarrollo.
- Se contemplarán los requisitos de Seguridad desde la fase de requisitos, en adelante.
- Se implementarán controles de seguridad dentro de los hitos del proyecto.
- Se utilizarán repositorios seguros.
- Se implementarán mecanismos de seguridad en el control de versiones.
- Los desarrolladores deberán tener la capacidad de evitar, encontrar y solventar vulnerabilidades.
- Durante el desarrollo, se deberá utilizar datos de prueba, y en caso de necesitar el uso de datos reales, se deberá utilizar técnicas que permitan ofuscar o enmascarar la información.

PROCEDIMIENTOS DE CONTROL DEL CAMBIO DEL SISTEMA

- Se asegurará que los cambios son aceptados por usuarios autorizados.

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas

- Se revisarán los controles y procedimientos de integridad para asegurar que no se comprometerán al realizar los cambios.

REVISIONES TÉCNICAS DE APLICACIONES TRAS REALIZAR CAMBIOS OPERATIVOS EN PLATAFORMA

- Se realizarán revisiones de control e integridad de la aplicación para asegurar que esta no ha sido comprometida por los cambios operativos en la plataforma.

- Se asegurará que la notificación de los cambios operativos en la plataforma se proporciona con la suficiente antelación para poder realizar pruebas y revisiones antes de la implementación.

- Se asegurará que los cambios pertinentes se realizan en los planes de continuidad del negocio existentes.

PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS

- Se deberá establecer procedimientos de ingeniería de sistemas que deberían establecerse, documentarse y aplicarse a las actividades relacionadas con la información de los sistemas de ingeniería.

- La seguridad deberá ser diseñada en capas de arquitectura, balanceando la necesidad de la seguridad de la Información con las necesidades de accesibilidad.

- La nueva tecnología debería analizarse para conocer sus riesgos de seguridad con la necesidad de accesibilidad.

- Los principios de ingeniería establecidos deberán aplicarse también a los sistemas externalizados a través de contratos y acuerdos con los proveedores.

ENTORNO DE DESARROLLO SEGURO

- Se deberán establecer entornos seguros para el desarrollo, considerando la sensibilidad de los datos que van a procesarse, almacenarse y transmitirse en el sistema.

- Se tendrán en cuenta los requisitos internos y externos aplicables, especialmente los de ámbito legal y contractual.

- Se podrán contemplar externalizaciones del desarrollo, pero también se deberá cumplir con las medidas de seguridad.

- Existirá control de acceso al entorno de desarrollo, deberán asegurarse la administración de operaciones sensibles o críticas en las aplicaciones desarrolladas permitiendo el uso de dobles factores de autenticación.

- Se deberá monitorizar los cambios en el entorno y del código almacenado en él.

- Las copias de seguridad se realizarán de forma regular y se almacenan en un sitio externo a la organización.

- Se controlará el movimiento de datos desde y hacia el entorno de desarrollo.

DESARROLLO EXTERNO

- Se deberán acordar de forma clara las licencias, la propiedad del código, así como los derechos de propiedad intelectual y la documentación relacionada.

- Se deberán acordar los requisitos contractuales para asegurar un diseño seguro, conforme a las prácticas de codificación y testeo.

- Se realizarán pruebas de aceptación y testeo, asegurando la calidad de los entregables.

- La estructura del entorno de desarrollo estará documentada, y se utilizará para crear los entregables.

VERFICACIÓN DE LA SEGURIDAD DEL SISTEMA

- Los sistemas nuevos actualizados se verificarán durante los procesos de desarrollo, incluyendo la preparación de actividades, tests de entrada, y las salidas esperadas sobre una serie de condiciones.

PRUEBAS DE ACEPTACIÓN DEL SISTEMA

- Las pruebas de aceptación del sistema deberán incluir los requisitos de verificación de seguridad de la información, así como cumplir con las prácticas de desarrollo de sistemas seguros.

- Las pruebas se realizarán tanto sobre componentes construidos o recibidos de forma externa, como sobre los sistemas integrados.

VERIFICACIÓN Y PROTECCIÓN DE LOS DATOS

- Los procedimientos de control de acceso que aplican a los sistemas operacionales de aplicación también se aplican sobre los sistemas de verificación y prueba.
- Deberá haber una autorización específica cada vez que se copian datos a un entorno de pruebas.
- La información operacional se borrará de los entornos de prueba tan pronto como se completen las pruebas.

5.17.- Política de relación con proveedores

Objetivo:

El objetivo de esta política es asegurar la protección de los activos de la organización que sean accesibles a proveedores, así como mantener un nivel acordado de seguridad y de provisión de servicios en línea con los acuerdos con los proveedores.

Contenido:

- Se deberán identificar todos los proveedores con los que existan relaciones contractuales.
- Se deberán de identificar y documentar los tipos de proveedores que guardan relación con la organización, y cuáles de ellos tienen acceso a la información de esta.
- Se definirá un proceso estandarizado y ciclo de vida para gestionar las relaciones con los proveedores.
- Se definirá los tipos de acceso a la información, en función del tipo de proveedores, y estos accesos se controlan y monitorizan.
- Para aquellos casos cuya dependencia del proveedor y su criticidad sea alta se establecerán acuerdos de nivel de servicio (ANS).
- Se definirá los mínimos requisitos de seguridad para cada tipo de información y de acceso, para que sirva como base de los acuerdos individuales con proveedores basados en las necesidades del negocio de la organización, sus requisitos, y su perfil de riesgos.
- Se establecerán controles para determinar la exactitud y competencia, asegurando la integridad de la información propia, del procesamiento de la información proporcionada por la otra parte.
- Se definirán los tipos de obligaciones aplicables a proveedores para proteger la información de la organización.
- Se establecerán acuerdos de Confidencialidad y de no divulgación para proteger la información confidencial por personal subcontratado y terceras partes.
- Se establecerán procesos y procedimientos para monitorizar el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y cada tipo de acceso.

5.18.- Política de monitorización y uso de los sistemas

Objetivo:

El objetivo de esta Política es la detección temprana de actividades y accesos no autorizados en los sistemas de Mnemo.

Contenido:

- Los sistemas de información y comunicaciones, bajo la responsabilidad de Mnemo, deberán mantener un registro de las operaciones que audite las actividades de la sesión.
- Los registros de la seguridad relacionados con las actividades se deberán mantener y conservar al menos durante tres meses.
- El Responsable de la Seguridad de la Información deberá revisar los registros con regularidad.
- Los relojes componentes de la red se deberán sincronizar con un servidor de tiempo de la red fiable.

5.19.- Política de seguridad sobre los aspectos de continuidad del negocio

Objetivos:

El objetivo de esta Política es establecer las directrices de la estrategia de contingencia ante incidentes o desastres en los sistemas que soportan los procesos de negocio de Mnemo. Dicha política incluirá planes, procedimientos y medidas que permitan la continuidad o el restablecimiento de la operatividad de los servicios de Mnemo ante un incidente o desastre. La continuidad en los servicios incluye generalmente uno o más de los siguientes enfoques para restablecer los servicios interrumpidos:

- Restableciendo las operaciones en una ubicación alternativa.
- Recuperar las operaciones utilizando sistemas alternativos.
- Ejecución de algunos o todos los procesos de negocio afectados utilizando medios manuales (sin sistemas de TICs). Esta opción sólo es aceptable para interrupciones muy cortas.
- Adopción de medidas de prevención de incidentes y desastres.

Contenido:

- Los planes de contingencia de sistemas deberán tener en cuenta los requisitos básicos del negocio, pero serán sus responsables quiénes deban desarrollar y mantener los Planes Globales de Continuidad del Negocio.
- Se desarrollará y mantendrá actualizado el Análisis de Impacto en el Negocio (BIA), como herramienta clave para determinar los sistemas que dan soporte a los procesos de negocio críticos, y por ello deberán incluirse en el Plan de Contingencia.
- Todos los procesos de negocio deberán de ser clasificados en categorías de criticidad, que indiquen el orden en que se recuperarán en caso de una interrupción del negocio, así como el período máximo durante el cual puede funcionar la empresa sin dichos procesos.
- Una vez elaborado el Plan de Continuidad de Negocio, se deberán establecer acciones de concienciación o simulacros periódicamente a todos los intervinientes, para garantizar la eficacia y eficiencia de su ejecución en el momento que sea necesario.

- Se deberán planificar una serie de pruebas del Plan de Continuidad de Negocio periódicas de modo que se analice la viabilidad y, al mismo tiempo, se puedan corregir deficiencias detectadas durante las pruebas.

- El Plan de Continuidad de Negocio deberá ser revisado, como mínimo anualmente, así como en aquellas ocasiones en las que se produzcan cambios en los sistemas y/o en la infraestructura.

- El Plan de Continuidad de Negocio deberá estar disponible para todos los intervinientes al menos en dos ubicaciones distintas.

- Los roles y las responsabilidades para un plan de emergencia y la recuperación de los sistemas de la información deberán de ser revisada y actualizada anualmente.

5.20.- Política de conformidad con los requisitos legales

Objetivos:

El objetivo de esta política es evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y al cualquier requisito de seguridad, garantizando que la seguridad de la información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales.

Contenido:

- Las exigencias y los reglamentos legales para cada sistema de la información deberán de ser documentados, con ello se pretende asegurar el cumplimiento con la legislación en vigor.
- Se deberá definir un procedimiento de vigilancia en materia legal por parte del responsable de Seguridad y DPO, con el objetivo de identificar:
    - Legislación aplicable a los sistemas de información y a su tratamiento.
    - Cambios legislativos que afecten a los sistemas de información
- El Responsable del SGSI es el encargado de asegurar que se realizan las auditorías establecidas por la legislación vigente en materia de seguridad de la información de Mnemo. Dichas auditorías comprenderán los requisitos legales, técnicos y organizativos.
- Los informes de auditoría de los sistemas de información serán analizados y custodiados conjuntamente por el Responsable de Seguridad y DPO, presentándose las conclusiones en el Comité de Calidad, Seguridad y Medioambiente.
- La organización deberá de obtener la autorización de las terceras partes antes de utilizar sus marcas comerciales.
- La organización deberá de identificar a los verdaderos propietarios de la información que utiliza si no posee los correspondientes derechos de autor.
- Al poner fin a una relación entre organización y cliente, toda la información concerniente al cliente deberá de ser archivada.

- Toda la información que no responda a las necesidades de la organización deberá de ser eliminada por las personas autorizadas.

- Toda la información concerniente a los incidentes de seguridad deberá ser conservada por la organización por un periodo de al menos tres años.

- El personal no está autorizado a proporcionar documentos o a atestiguar sobre los hechos concernientes sobre un incidente de seguridad a terceras partes. En el supuesto de haber recibido una citación judicial, y con carácter previo a cualquier actuación al respecto, es obligatorio dirigirse al Responsable de Seguridad, que decidirá sobre las actuaciones a realizar.

- Cualquier información que no aparezca en el criterio de retención de la organización se deberá conservar tanto tiempo como sea posible en un lugar seguro.

- Los análisis forenses informáticos deberán ser realizados en copias para preservar la integridad de la evidencia. La evidencia original se deberá de mantener en un lugar seguro.

- Toda la información relevante, sujeta a cumplimiento normativo, legislativo, contractual, ect. de la organización deberá de ser almacenada por un periodo de tiempo determinado, establecido según la normativa aplicable a cada dato y/o supuesto.

- La documentación en formato papel deberá ser destruida, o bien mediante las destructoras de papel ubicadas en las instalaciones o bien rompiéndolas (siempre que no sea información confidencial o de uso interno).

- Las investigaciones internas de los incidentes de seguridad de la información deberán de ser llevadas a cabo por el Área de Inteligencia. El personal deberá responder a las preguntas del Área de inteligencia de Mnemo durante las investigaciones.

- La investigación de la actividad criminal es confidencial. Los resultados no pueden ser desvelados antes de que las acusaciones sean formuladas o se hayan tomado las medidas disciplinarias adecuadas.

- Es necesaria la autorización de los clientes y de las terceras partes antes de obtener información confidencial sobre ellos. Está prohibida la venta o cambio de esta información.

- Está terminantemente prohibida la venta, el alquiler, el intercambio o cualquier otra forma de transferir información personal de los clientes y/o de cualquier persona física.

- Los clientes deberán ser informados cuando su información personal sea manejada por otra organización, cuando la organización sufra una fusión o una adquisición por otra organización.

- Es necesaria la autorización de la organización, proveedor o cliente antes de divulgar su información a terceros. Por otra parte, se deberá de guardar un registro de las cesiones de información a terceras partes.

- Los empleados deberán de estar informados de que la organización puede efectuar una verificación, sin previo aviso, de toda la información almacenada en su sistema de la información.

- Si se produce un incumplimiento referente a las políticas de Mnemo o si encuentra información comprometedora, no permitida en su repositorio o dispositivo móvil, el empleado deberá tener la posibilidad de dar una explicación.

- La recolección de información privada se deberá realizar por medios legales y sólo para cubrir el interés legítimo de la organización.

- Las razones que conducen al despido de un empleado solamente se divulgarán a las personas autorizadas.

6.- Documentación de referencia

- UNE-EN ISO/IEC 27001:2014 Sistema de gestión de seguridad de la información.
- UNE-EN ISO/IEC 27002:2017 Código de prácticas para los controles de seguridad de la información.
- ISO/IEC 20000-1:2018 Sistema de gestión de servicios
- ISO/IEC 22301:2019 Sistema de gestión de continuidad del negocio
- ISO/IEC 27701:2019 Sistema de gestión de información privada
- Esquema Nacional de Seguridad, Real Decreto 951/2015

7.- Documentación relacionada

- FG-07.04.01 Comunicaciones.
- MSI-02 Responsabilidades de seguridad de la información