ÍNDICE

REVISIONES DEL DOCUMENTO		
VERSIÓN	FECHA	MODIFICACIÓN
1	02/12/2024	Creación del documento para adaptación Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Editado por:	Revisado por:	Aprobado por:	Fecha
Miguel Ángel de San José Moreno	*Benjamín Caro Magunacelaya*	*Benjamín Caro Magunacelaya*	02/12/24

1 Objeto

Meydis desarrolla la presente Política de Seguridad, con la finalidad de establecer las directrices que van a regir la forma en que el Meydis gestiona y protege la información que trata y los servicios que presta.

La seguridad de los sistemas de Meydis estará basada en los siguientes principios:

- Un **proceso integral** entendido como un sistema organizativo y técnico completo que aúne recursos humanos, materiales, institucionales y legales y se sustente en una adecuada concienciación y formación del personal, en función de la forma en la que participe en el mismo para poder, así, reducir al máximo la ocurrencia de incidencias por errores humanos debidos a desconocimiento o ausencia de organización. Este proceso integral de seguridad será actualizado y mejorado de forma continua.
- Una adecuada y continua **gestión de la seguridad basada en los riesgos** identificados y que establezca medidas para su tratamiento, que permitan reducir estos para que puedan ser más fácilmente controlados y alcancen niveles aceptables.
- Una eficaz **gestión de incidentes** con los siguientes objetivos:
    - Prevenir, en la manera de los posible, que las amenazas se materialicen en sus sistemas de tratamiento y que se conviertan en incidentes de seguridad
    - Establecer un procedimiento robusto de detección de vulnerabilidades que le aporte información temprana de los riegos a los que se encuentran expuestos los sistemas de tratamiento, y se pueda, así, adoptar un elenco de medidas preventivas.
    - Dar una adecuada y rápida respuesta a los incidentes acaecidos que posibilite que estos se detengan y que sean aislados para acabar, lo antes posible, con los daños que estén causando o puedan causar en la infraestructura o información y aislar los mismos de los demás elementos del sistema.
    - Preservar los datos e información para garantizar su disponibilidad.
- Un diseño e implantación de diferentes **capas de seguridad** a distintos niveles que permitan defender los ataques a sus sistemas mediante barreras de obstáculos, que un ciberdelincuente tendría perpetrar correlativamente antes de poder acceder a su infraestructura o información, protegiendo en último caso su núcleo duro y permitiendo aislar el ataque antes de que llegue al mismo.

- Diferentes **procesos de supervisión, evaluación** y, en su caso, **monitorización** con la finalidad de detectar anomalías y de reajustar y redefinir las medidas de seguridad implantadas en el sistema para que estas sean eficientes y eficaces, en todo momento, y se ajusten a la evolución tecnológica y los nuevos riesgos que comprometan a la seguridad de los sistemas.
- Una robusta **segregación de funciones y responsabilidades** de las personas claves en la gestión de la seguridad.

La seguridad de la información de Meydis estará basada en los siguientes principios:

- Asegurar la **confidencialidad** de la información, impidiendo accesos indebidos y garantizando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización para ello.
- Mantener la **integridad** y exactitud de la información, consiguiendo que no se produzcan modificaciones no autorizadas.
- Garantizar la **disponibilidad** de la información y que puedan acceder a ella las personas autorizadas.
- Asegurar la **autenticidad** de la información, comprobando que la fuente de origen es adecuada o que la persona de origen es quién dice ser.
- Preservando la **trazabilidad** y que las acciones puedas ser imputables a sus autores.

2 Alcance y propiedad

Esta política aplica a todo Meydis a todos sus miembros y a todos sus activos:

- Personal propio y subcontratado.
- Clientes, proveedores y colaboradores.
- Infraestructura física y lógica.
- Soportes físicos y lógicos.
- Información y datos.
- Servicios y procesos.

El propietario y responsable de implantar la presente Política es la alta Dirección de Meydis.

3 Descripción

3.1 Organización de la Seguridad

La estructura organizativa mínima en el ámbito de la seguridad de la información de Meydis será la siguiente:

- La Comisión de seguridad del Comité de Gestión Integrada (en adelante, Comisión de seguridad).
- Los Responsables de la información y de los servicios.
- El Responsable de Seguridad.
- El Responsable del sistema de información.

Para su determinación se ha tenido en cuenta la guía de seguridad (CCN-STIC-801) Responsabilidades y funciones.

El nivel al que actúa la Comisión de seguridad y el personal cualificado en materia de seguridad es el siguiente;

	Nivel de gobierno	**Nivel de supervisión**	**Nivel operativo**
Comisión de seguridad	**X**	**X**	
Responsables de la Información y de los Servicios	**X**		
Responsable de Seguridad		**X**	
Responsable del Sistema de Información			**X**

3.1.1 Comisión de seguridad

Con la finalidad de coordinar la seguridad de la información, Meydis crea una Comisión de seguridad compuesta por un equipo multidisciplinar.

A -. Funciones

La Comisión de seguridad tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de Meydis y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- 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.

La Comisión de seguridad deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

- Grupos de trabajo especializados, internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de eventos formativos o de intercambio de experiencias.

El Responsable de la Seguridad será el secretario de la Comisión de seguridad, y como tal:

- Convocará sus reuniones.
- Preparará los temas a tratar en las reuniones, aportando información puntual para la toma de decisiones.
- Elaborará el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones de la Comisión.

B -. Nombramientos

La dirección de Meydis deberá nombrar a los siguientes miembros de la Comisión de seguridad:

- Al los Responsables del servicio y de la información.
- Al Responsable de la Seguridad.
- Al Responsable del sistema de información.

Además, la Comisión de seguridad podrá estar formado por otros miembros que sus miembros o la dirección de Meydis considere oportuno.

Los miembros de la Comisión serán designados en un documento de nombramiento o el acta de la Comisión correspondiente, donde deberán aceptar las funciones y responsabilidades derivadas de dicha designación.

La identidad de los miembros de la Comisión de seguridad será comunicada a todos los miembros de Meydis mediante correo electrónico.

C -. Estructura

La estructura de la Comisión de seguridad será la siguiente:

- Presidente: Miembro de la dirección.
- Vocales:
  - Los Responsables de la información y de los servicios.
  - Responsable del sistema de información.
  - Otros miembros convenientemente designados.
- Secretario: Responsable de Seguridad.

D -. Dinámica de reuniones

La Comisión de seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

3.1.2 Responsable de la información y del servicio

Son miembros pertenecientes a la dirección de Meydis y las personas que ostentan la responsabilidad unificada de establecer los requisitos del servicio y de la información que estos tratan en materia de seguridad.

Los Responsables de la información y de los servicios son los encargados, a nivel de gobierno, de velar por el cumplimiento de la normativa de seguridad definida por MEYDIS en los servicios identificados y de los que son responsables, respectivamente.

Son funciones de los Responsables de la información y del servicio:

- Determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).
- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.
- Realizar los análisis de riesgos, y de seleccionar las salvaguardas a implantar contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del sistema de información.
- Aceptar los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control.

Los Responsables de información y de los servicios serán convenientemente nombrados y cesados por la Comisión de seguridad.

Los reportes y flujo de información se realizarán de la siguiente forma: los Responsables de la información y del servicio reportarán al Responsable de Seguridad y, en su caso, a los clientes de sus servicios, las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dichos servicios.

3.1.3 Responsable de Seguridad

El Responsable de Seguridad determina, a nivel de supervisión, las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

Las funciones esenciales del Responsable de Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la presente Política de Seguridad.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El resto de las funciones del Responsable de Seguridad que podrán ser, en su caso, delegadas son:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con las autoridades competentes en materia de seguridad de las redes y sistemas de información.

- Notificar a las autoridades competentes los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías de seguridad, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Todas aquellas funciones que específicamente se determinen en el documento de su nombramiento.

Además, el Responsable de Seguridad será el POC (Punto o Persona de Contacto) para la seguridad de la información tratada y los servicios prestados a las entidades del sector público, con la finalidad de canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio prestado o solución comercializada, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

La figura del POC podrá ser delegada en una persona que forme parte de del área del Responsable de Seguridad o que tenga comunicación directa con la misma.

El Responsable de Seguridad será nombrado y cesado por la Comisión de seguridad.

Los reportes y flujo de información se realizarán de la siguiente forma:

- El Responsable de la Seguridad reportará al Responsable de la información y del servicio las decisiones e incidentes en materia de seguridad que afecten a la información y servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- El Responsable de la Seguridad informará a la Comisión de seguridad e informará a la dirección de Meydis, entregándoles un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

3.1.4 Responsable del Sistema de información

El Responsable del Sistema, por sí o a través de recursos propios o contratados, se encargará de 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.

El Responsable del Sistema, a nivel de operación, tendrá las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Aprobación de los procedimientos técnicos, bajo la supervisión del Responsable de Seguridad.
- Generación de Informes, registros y evidencias electrónicas.

El Responsable del Sistema de Información será nombrado y cesado por La Comisión de seguridad.

Los reportes y flujo de información se realizarán de la siguiente forma:

- El Responsable del sistema de información reportará al Responsable de la información y del servicio sobre las incidencias funcionales relativas a la información y servicio que le compete.
- El Responsable del Sistema reportará al Responsable de la Seguridad de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema y le entregará un resumen consolidado de los incidentes de seguridad.

3.1.5 Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

3.2 Identificación de la legislación aplicable

Meydis declara su absoluto compromiso con el cumplimiento de las leyes, reglamentos y normas aplicables a su sistema de gestión de la seguridad de la información.

Meydis debe identificar los requisitos legales, regulatorios y normativos que afectan a su organización y, en concreto, a su sistema de gestión de la seguridad de la información, para dar cumplimiento a los mismos y no

verse expuesto a riesgos innecesarios por desconocimiento de sus obligaciones.

Para ello el Responsable de Seguridad será el encargado de identificar la legislación aplicable, solicitando auxilio a sus proveedores especializados en las diferentes materias (abogados, consultores, DPO) y registrando la misma en el RG-Repositorio de legislación, PG, PLS, ITS y guías CCN-STIC-CNN-CERT-Meydis. Dicho repositorio será revisado, al menos una vez año, por el Responsable de Seguridad y actualizado, por el mismo, cada vez que haya un cambio legislativo, regulatorio o similar.

El Responsable de Seguridad, a través de la normativa de seguridad correspondiente, deberá comunicar el obligado cumplimiento de la legislación aplicable a su personal y a las partes interesadas.

3.3 Protección de datos y privacidad de la información personal

Meydis trata datos de carácter personal en estricto cumplimento de la legislación en materia de protección de datos de carácter personal aplicable.

La documentación exigida por el RGPD y la LOPD-GDD especifica los tratamientos de datos personales realizados por Meydis y las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos que afectan a dichos tratamientos. La referida documentación de encuentra a disposición de los usuarios en la intranet.

Los principales riesgos que afectan a los tratamientos realizados por Meydis se han identificado como los siguientes:

- La pérdida de la Confidencialidad (acceso no autorizado), Integridad (modificación o alteración de los datos no intencionada) y Disponibilidad (pérdida de datos).
- A su vez, representa un riesgo asociado el cumplimiento de los requisitos legales relacionados con los derechos y libertades de los interesados (uso ilegítimo de datos personales o imposibilidad de cumplir las obligaciones exigidas por la legislación de protección de datos).

Meydis basará la seguridad de la información personal que maneja en proteger la misma de los referidos riesgos.

3.4 Análisis y gestión de riesgos

Meydis asume el compromiso de controlar los riesgos a los que están sometidas sus entidades mediante la realización de análisis de riesgos en intervalos planificados y la gestión de los mismos de una forma eficaz.

Para la realización de los referidos análisis de riesgos, Meydis utilizará alguna metodología específica en base a un catálogo básico de amenazas y una semántica definida.

La metodología utilizada tendrá como finalidad identificar las amenazas a las que están sometidos los activos críticos del sistema de información de Meydis, las vulnerabilidades y salvaguardas de los mismos y, como consecuencia, los riesgos asociados a la perdida de la disponibilidad, integridad y confidencialidad de la información que tratan.

Dichos riesgos serán valorados sobre las variables de la probabilidad y el impacto de que estas amenazas se aprovechen de las vulnerabilidades, que no han sido convenientemente tratadas con las correspondientes salvaguardas, y se materialicen en el sistema de información.

Una vez identificados los riesgos, estos serán gestionados determinando los niveles aceptables y tratando todos aquellos que superen el umbral establecido por la Dirección.

El tratamiento de dichos riesgos se plasmará en un plan de tratamiento de riesgos en el que se detallarán las salvaguardas o medidas de seguridad a implantar, se identificarán a los responsables, se establecerán los plazos para su implantación y se detallarán los recursos necesarios. Las salvaguardas o medidas de seguridad a implantar para mitigar o suprimir los riesgos estarán justificadas y, en todo caso, existirá proporcionalidad entre ellas y los riesgos.

Dicho análisis de riesgos y plan de tratamiento deberán ser revisados anualmente, siempre que se produzcan modificaciones sustanciales en el sistema de información de Meydis y en el caso que se produzca algún incidente grave.

3.5 Desarrollo de la Política de Seguridad

Como materialización del compromiso de la alta Dirección de Meydis respecto al sistema de gestión de la seguridad de la información se ha establecido en la presente política de seguridad documentada, que debe

ser comunicada a todo el personal interno y estar disponible para las partes interesadas.

Se ha tenido en cuenta para su desarrollo, lo establecido en guía de seguridad (CCN-STIC-805).

La presente Política de seguridad de la información (PSI) se apoya en normativa sobre temas específicos que profundizan en la implantación de las medidas de seguridad y que están estructuradas para atender las necesidades de determinados grupos dentro de la organización y cubrir ciertos temas.

La normativa será clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- **Primer nivel**: Política de seguridad de la información (PSI).
- **Segundo nivel**: Procesos de gestión (PG) y Políticas o normativa de Seguridad (PLS).
- **Tercer nivel**: Procedimientos de Seguridad (PRS-IT).
- **Cuarto nivel**: Informes, registros y evidencias electrónicas (RG).

Primer Nivel.- Política de Seguridad: De obligado cumplimiento por todo el personal, interno y externo, de Meydis, recogido en el presente documento. La responsabilidad de aprobación será de la alta Dirección.

Segundo Nivel.- Normativas: De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia de la Comisión de Seguridad o del Responsable de Seguridad, bajo la supervisión del primero, o de un miembro en su representación.

Tercer Nivel.- Procedimientos de Seguridad: Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del sistema de información correspondiente, bajo la supervisión del Responsable de Seguridad.

Cuarto Nivel.- Informes, registros y evidencias electrónicas: Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información. La responsabilidad de que existan este tipo de documentos es del Responsable del sistema de información.

Las Políticas de Seguridad sectoriales dependientes de la presente Política de seguridad de la información de Meydis son las siguientes:

- PLS-02 Política de seguridad en los Recursos Humanos.
- PLS-03 Política de tratamiento de la información y gestión de activos.
- PLS-04 Política de control de acceso.
- PLS-05 Política de seguridad física y del entorno.
- PLS-06 Política de seguridad en la relación con clientes.
- PLS-07 Política de seguridad en la relación con proveedores.
- PLS-08 Política de gestión de incidencias.
- PLS-09 Política de continuidad de negocio.
- PLS-10 Política de seguridad de sistemas.
- PLS-11 Política de criptografía.

Los roles, responsabilidades y autoridades dentro de la organización y en materia de seguridad, se encuentran detalladas en las referidas políticas de Seguridad de Meydis, en su epígrafe "Funciones y responsabilidades" con el que todas ellas cuentan, y en la presente Política.

Gestión

El sistema de gestión de la seguridad de la información de Meydis es planificado, operado, evaluado y mejorado según lo establecido en los procesos de gestión de calidad y seguridad de la organización.

Todas las actuaciones requeridas para la correcta gestión de la seguridad en Meydis se encuentran detalladas en los siguientes procesos de gestión de calidad y seguridad de la organización:

- PG1 - Proceso de liderazgo.
- PG2 - Proceso de contexto de la organización.
- PG3 - Proceso de gestión de riesgos.
- PG4 - Proceso de apoyo.
- PG5 - Proceso de información documentada.
- PG6 - Proceso de seguimiento, medición, análisis y evaluación.

- PG7 - Proceso de no conformes y acciones.
- PG8 - Proceso de auditoría interna.
- PG9 - Proceso de revisión por la dirección.
- PG10 - Proceso de análisis y gestión del riesgo de sistemas de información.
- PG11 - Proceso de análisis y gestión del riesgo de sistemas de información-ENS.

Distribución

Los procesos, políticas y resto de normativa aplicable al sistema de información estarán disponible para todos los usuarios en la intranet y será aplicable a los usuarios de acuerdo con lo establecido en el RG-Repositorio de legislación, PG, PLS, ITS y guías CCN-STIC-CNN-CERT-Meydis", en función de los establecido en los apartados "Alcance y propiedad" de cada uno de los documentos que la conforman.

3.6 Obligaciones y gestión del personal

Todos los miembros de Meydis tienen la obligación de conocer y cumplir esta Política de seguridad de la información y la normativa de desarrollo, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los interesados.

Meydis asume el compromiso de formar e informar a todos sus miembros de sus deberes y obligaciones en materia de seguridad.

Las actuaciones de los miembros de Meydis deberán ser supervisadas, en intervalos planificados, para verificar que se siguen los procedimientos de seguridad establecidos y que respetan los principios de seguridad establecidos en la presente Política de Seguridad.

Los deberes y obligaciones en materia de seguridad de los miembros de Meydis deberán ser necesariamente plasmados en normativa de seguridad.

Con la finalidad de poder depurar responsabilidades en el cumplimiento de deberes y obligaciones en materia de seguridad, cada usuario de Meydis que acceda a la información del sistema será identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

3.7 Terceras partes

Meydis hará partícipes de esta Política de seguridad de la información a las entidades públicas y privadas a las que preste servicios o de las que maneje información.

El Comité de Seguridad establecerá los canales para el reporte y coordinación de la seguridad con los referidos clientes y los procedimientos de actuación para la reacción ante incidentes de seguridad.

A su vez, Meydis también hacer partícipes de esta Política y de la normativa de seguridad correspondiente, a los terceros de los que utilice servicios o a los que comunique información.

Dichos proveedores quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de los referidos proveedores esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

3.7.1 Contacto con las autoridades

La dirección de Meydis se compromete, como parte de la estrategia definida para cumplir con sus objetivos en materia de seguridad, mantener los contactos oportunos con las siguientes autoridades y mantenerles informados de los incidentes de seguridad en los términos exigidos por la legislación aplicable:

AUTORIDADES Y SUS DATOS DE CONTACTO					
Organismo	**Propósito**	**URL de comunicación**	**Dirección postal**	**Teléfono**	**Correo electrónico**
AEPD Agencia Española de Protección de datos	Comunicación de **brechas de seguridad o consultas**	https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguri	C/ Jorge Juan, 6, 28001-Madrid	901 100 099 912 663 517	dpd@aepd.es

	sobre tratamiento de **datos personales**	dad/procedimientoBrechaSeguridad.jsf			
Policía Nacional - **Brigada de Investigación Tecnológica**	Comunicación delitos tecnológicos y consultas relativas	https://www.policia.es/_es/colabora_informar.php?strTipo=CGPJDT	C/ Julián González Segador s/n, 28043 - Madrid	91 5822747	delitos.tecnologicos@policia.es
Guardia Civil: **Delitos Telemáticos (GDT)**	Comunicación y consultas relativas a delitos informáticos	https://www.gdt.guardiacivil.es/webgdt/pinformar.php	C/ Guzmán el Bueno, 110, entr., C.P. 28003, Madrid	062	sugerencias@guardiacivil.org
INCIBE-CERT	Comunicación de incidentes cuando se presten servicios digitales a la AAPP				incidencias@incibe-cert.es.

3.7.2 Contacto con grupos de especial interés

La dirección de Meydis se compromete, como parte de la estrategia definida para cumplir con sus objetivos en materia de seguridad, mantener los contactos oportunos con grupos específicos que proporcionen información actualizada en materia de seguridad relativos a los recursos que componen su sistema de información, con la finalidad de detectar, de forma temprana, nuevas amenazas y vulnerabilidades y de conocer, lo antes posible, las herramientas, parches y buenas prácticas que pueden contener o tratar las mismas.

Sin ser una lista cerrada, Meydis estará al día de la información que proporcionen los siguientes grupos de interés:

GRUPOS DE INTERES Y TIPO DE CONTACTO		
Grupo	**Propósito**	**Tipo de contacto**
INCIBE-CERT	Estar al día de los incidentes de seguridad y vulnerabilidades que afectan a los diferentes fabricantes y productos utilizados por la entidad.	Suscripción a su Newsletter de avisos y vulnerabilidades, a través de: https://www.incibe-cert.es/en/newsletter/subscriptions?opcion=si
CN-CERT	Estar al día de las vulnerabilidades que afectan a los diferentes fabricantes y productos utilizados por la entidad.	Consulta periódica a la página https://www.ccn-cert.cni.es/
UNA AL DIA - HISPASEC	Estar al día de las vulnerabilidades que afectan a	Suscrición a su Newsletter de vulnerabilidades, que se recibe

	los diferentes fabricantes y productos utilizados por la entidad.	desde la cuenta de correo - noticias@hispasec.com
MICROSOFT	Estar al día de las vulnerabilidades que afectan a los diferentes fabricantes y productos utilizados por la entidad.	Suscrición a su Newsletter de vulnerabilidades, que se recibe desde la cuenta de correo - PowerPlat-noreply@microsoft.com
QNAP	Estar al día de las vulnerabilidades que afectan a los diferentes fabricantes y productos utilizados por la entidad.	Suscrición a su Newsletter de vulnerabilidades, que se recibe desde el dominio - https://www.qnap.com/solution/notification-center/es-es/
FORTINET	Estar al día de las vulnerabilidades que afectan a los diferentes fabricantes y productos utilizados por la entidad.	Suscrición a su Newsletter de vulnerabilidades, que se recibe desde la cuenta de correo - noreply@fortinetpm.com

En relación con los servicios en la nube, serán los propios proveedores los que notificarán las brechas de seguridad y vulnerabilidades encontradas a los Administradores de cada plataforma o herramienta y/o publicarán las mismas en sus portales de transparencia.

3.8 Publicación y comunicación de la política de seguridad partes

La presente Política de Seguridad será comunicada de la siguiente forma:

- A todos los miembros de Meydis mediante correo electrónico y su publicación en la intranet.
- A los terceros interesados mediante su publicación en la página web de Meydis.

Esta política entrará en vigor al día siguiente de su aprobación y sustituye a la anterior PLS-01 Política de Organización Interna y Cumplimiento Legal, derivada del SGSI.

La Responsable de Seguridad será el encargado de realizar dicha comunicación y puesta a disposición de la presente Política.

4 Funciones y responsabilidades

Alta Dirección

- Analizar el contexto en el que se va a desarrollar el sistema de gestión y comprender las necesidades del mismo.
- Liderar y comprometerse con el sistema de gestión de la seguridad de la información.
- Determinar y revisar el alcance del sistema de gestión de la seguridad de la información.
- Participar en la planificación, operación, evaluación y mejora continua del sistema de gestión, según lo establecido en los procesos de gestión.
- Nombrar y, en caso, cesar a los miembros de la Comisión de seguridad y los puestos claves.
- Comunicar a los usuarios la legislación aplicable.

Comisión de seguridad

- Realizar las actuaciones descritas en el epígrafe 3.1 Organización de la Seguridad.

Responsable de la información y de los servicios

- Realizar las actuaciones descritas en el epígrafe 3.1 Organización de la Seguridad.

Responsable de Seguridad

- Realizar las actuaciones descritas en el epígrafe 3.1 Organización de la Seguridad.
- Identificar, registrar y actualizar la legislación aplicable.
- Comunicar y poner a disposición de la presente Política.

Responsable de Sistema de información

- Realizar las actuaciones descritas en el epígrafe 3.2 Organización de la Seguridad.

Usuarios

- Cumplir con lo establecido en la presente Política, su normativa de desarrollo y la legislación aplicable, en los términos que le hayan sido exigidos por la organización y en lo que afecte al desarrollo de sus funciones.

5 Documentos aplicables

- Toda la normativa de la organización.
- Guía de seguridad (CCN-STIC-805) - esquema nacional de seguridad política de seguridad de la información.
- Guía de seguridad (CCN-STIC-801) responsabilidades y funciones.
- RG-Repositorio de legislación, PG, PLS, ITS y guías CCN-STIC-CNN-CERT-Meydis.

6 Anexos

- Esta política no dispone de Anexos.