POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esquema Nacional de Seguridad- ISO 27001- Reglamento Europeo 2016/679- L.O.P.D.G.D.D. 3/218

Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS- C.I.F.: G29830643

Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina -IBIMA Plataforma BIONAND-

Calle Severo Ochoa, 35; Parq. Tecn. de Andalucía (PTA) Campanillas, Málaga 29590.

tlf. 951 440 260- 951 440 263 / fimabis@fimabis.org / ibima@ibima.eu

FIMABIS

Contenido

1. INTRODUCCIÓN....4
2. OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN....4
2.1.- ÁMBITO Y ALCANCE GENERAL....5
2.2.- ÁMBITO ESPECÍFICO ENS....8
3. OBJETIVOS Y MISIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN....9
4. ALCANCE....11
5. MARCO LEGAL Y NORMATIVO....12
5. AUTORIDAD SOBRE LA POLÍTICA Y REVISIÓN....13
6. ORGANIZACIÓN DE LA SEGURIDAD....13
6.1. ROLES Y RESPONSABILIDADES....14
6.1.1. Usuarios/as....14
6.1.2. Responsable de la Información....14
6.1.2. Responsable de la Seguridad y servicio....15
6.1.3. Responsable y administrador de los sistemas....16
6.1.4.- Asesor jurídico y Compliance....17
6.1.5. Delegado de Protección de Datos....17
6.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES....18
7. ÁMBITOS DE GESTIÓN CUBIERTOS POR LA POLITICA....19
7.1. ANÁLISIS Y GESTIÓN DE RIESGOS....19
7.2. PLANIFICACIÓN y METODOLOGÍA....19
7.3. CONTROL DE ACCESOS....20
7.4. EXPLOTACIÓN....21
7.5. SERVICIOS EXTERNOS....22
7.6. CONTINUIDAD....22
7.7. MONITORIZACIÓN....23
7.8. INSTALACIONES E INFRAESTRUCTURAS....23
7.9. PERSONAL, CONCIENCIACIÓN Y FORMACIÓN....23
7.10. EQUIPAMIENTO Y RESPONSABILIDADES DEL USUARIO....24
7.11. COMUNICACIONES....24
7.12. SOPORTES DE INFORMACIÓN....25
7.13. APLICACIONES....25
7.14. INFORMACIÓN....25
7.15. VIGILANCIA CONTINUA....26
8. DESARROLLO Y DESPLIEGUE DE LA POLÍTICA DE SEGURIDAD....26
8.1. INSTRUMENTOS DE DESARROLLO....26
8.2. SANCIONES PREVISTAS EN CASO DE INCUMPLIMIENTO....27

ANEXOS **27**
A.1.- Constitución Comité Seguridad **27**
A.2.- Declaración de Aplicabilidad **27**
B.1.- Gestión acreditativa ENS **27**
B.2.- Gestión acreditativa L.O.P.D.G.D.D. **27**

CONTROL DE VERSIONES:

	REALIZADO:	REVISADO:	APROBADO:
Reg. Versión	Versión 1	Versión 1	Versión 1
FECHA	20/06/2024	23/07/2024	23/07/2024
NOMBRE	José Montilla Chicano	Comité Seguridad de la Información	Comité Seguridad de la Información
CARGO	DPD (Externo)		
FIRMA			

Lugar de archivo: Centauro		
Responsables custodia: Eva Pena		
Fecha de revisión 23/07/2026		
Registro histórico de versiones		
Versión 1		Edición Inicial

1. INTRODUCCIÓN

Este documento expone la Política de Seguridad de la Información de Fundación para la Investigación de Málaga en Biomedicina y Salud -FIMABIS-, como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la seguridad en el tratamiento de la información, recogiendo las exigencias del Reglamento Europeo 216/679 y la Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales 3/2018, así como el Esquema Nacional de Seguridad (ENS) y la norma ISO 27001.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de FIMABIS Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de FIMABIS.

La dirección de FIMABIS, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento. Para dar cumplimiento a dicha obligatoriedad de proactividad en la seguridad de los tratamientos de la información, FIMABIS ha aprobado la presente política de seguridad de la información para la protección de sus sistemas de información conforme al alcance definido para el sistema de gestión de seguridad de la información para cada una de las normas a las que se ha hecho referencia.

La entrada en vigor de la presente Política de Seguridad de la Información de FIMABIS sustituye cualquier otra que existiera a nivel de los diferentes departamentos o áreas de la organización.

2. OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN

La **Fundación para la Investigación de Málaga en Biomedicina y Salud** -FIMABIS- y el **Instituto de Investigación Biomédica de Málaga y Plataforma en Nanomedicina** -IBIMA Plataforma BIONAND- es una organización dedicada al desarrollo de la docencia, la investigación científica y el desarrollo tecnológico en Ciencias de la Salud, así como la promoción y mejora de la asistencia sanitaria pública.

FINALIDADES:

- ✓ Promover una investigación biomédica de excelencia y orientada a resultados en salud.
- ✓ Alentar la colaboración entre los equipos de investigación de los centros del Sistema Sanitario Público de Andalucía y el resto de los agentes del Sistema de Ciencia Tecnología Empresa
- ✓ Facilitar el acceso de los investigadores a nuevas vías de financiación de sus investigaciones
- ✓ Promover la realización de actividades docentes y de formación continuada
- ✓ Promover la edición de publicaciones de carácter científico

- ✓ Canalizar los recursos materiales y dar soporte administrativo a los procedimientos de selección de profesionales y de contratación o adquisición de bienes o equipos que les sean concedidos a los proyectos de investigación en salud cuya gestión les sea encomendada.
- ✓ Conceder becas y ayudas económicas para el desarrollo de proyectos de investigación y la adquisición de equipos necesarios para llevarlos a término
- ✓ Incrementar la eficiencia de las estructuras de apoyo y gestión de la investigación
- ✓ Diseñar, desarrollar y gestionar proyectos y centros de investigación e innovación
- ✓ Contribuir a la gestión eficiente del conocimiento y los resultados generados en las actividades de investigación e innovación
- ✓ Desarrollar actuaciones que contribuyan a la puesta en común de conocimientos y a la difusión de la Ciencia y Tecnología
- ✓ Potenciar la asistencia sanitaria pública a través de cualquier medida o actuación que redunde en su mejora

2.1.- ÁMBITO Y ALCANCE GENERAL

2.1.1.- TIPOLOGÍA DE DATOS Y COLECTIVOS

Las citadas actividades determinan como áreas y ámbito de información:

1.- TIPOLOGÍA DE DATOS Y COLECTIVOS

En base a su objeto social se determinan como áreas y ámbito de información:

I.- Área Investigación y Formación

I.i.- Gestión proyectos.

a) Tratamiento de datos personales de usuarios/as, necesarios para la investigación biomédica con inclusión de datos identificativos, de salud, e imagen.

Son proporcionados por Investigador/a Principal (IP) y los servicios clínicos del SAS adscritos a los proyectos de investigación, con consentimiento informado de interesado/a, no se contempla cesión ni comunicación directa, siendo sometidos a procesos de seudonimización efectiva, por parte de IP y SAS para su tratamiento, lo que confiere carácter anonimizado.

b) Tratamiento de datos bajo finalidad de investigación y/o formación

I.2. Gestión personal.

I.1.- Tratamiento de datos personales de investigadores y colaboradores, personal vinculado a investigación y formación, con inclusión de datos identificativos, de contacto, y curriculares, con inclusión de imagen.

Son proporcionados por el propio interesado en base a su relación con la Entidad, y pueden ser cedidos/comunicados a las distintas entidades vinculadas, SAS, Universidad de Málaga, así como a otras relacionadas con la investigación y/o formación, y aquellas derivadas de obligaciones legales.

I.2.- Tratamiento de datos bajo finalidad de control y gestión de la investigación y/o formación

I.3.- Tratamiento de datos bajo finalidad de gestión de eventos y actividades promocionales, con posible inclusión de datos de personal responsable, y datos personales de participantes. Con cesión a entidades convocantes y empresas aseguradoras.

II.- Área de Gestión Corporativa

Tratamiento de la información necesaria para la gestión y desarrollo de la propia Entidad

1. **Área Administrativa-Económica**: Control y fiscalización interna de la gestión económico-financiera, presupuestaria y tesorería de la entidad, abarcando las funciones contables, tributarias, fiscales y todas las relativas, en general, a la planificación económica.
    - **Ficheros de Gestión Administrativa-Económica**: estructura general de actividades administrativas, contabilidad/facturación, proyectos, proveedores, etc., Reseñándose datos de identificación, domicilio, servicios prestados, datos bancarios de alumnado y representantes legales. Datos en parte empresariales.

Nivel de Seguridad Básico. Se comunica a la administración competente tributaria y fiscal.

2. **Área Jurídica**: Estudio, asesoramiento jurídico y propuestas de carácter superior, preparación de los asuntos a estudiar por los órganos resolutivos y actuaciones en materia de gestión laboral e investigadora.
    - **Ficheros generados en el departamento jurídico**, con tratamiento de posibles reclamaciones y cuestiones legales de personal laboral y colaborador vinculado, órganos de dirección y gestión. Acceso restringido al responsable Jurídico, con comunicación a Comisiones competentes, así como administración correspondiente.
3. **Área Recursos Humanos y Organización**: Estudio, informe, gestión, asesoramiento y propuesta en materia de recursos humanos y su formación, así como medidas organizativas de la misma.
    - **Fichero Gestión Laboral y Recursos Humanos**: gestión y tratamiento de los datos de personal, nóminas y curriculum. Servicios de prevención de Riesgos Laborales. Se comunica a la Administración competente, Servicio Empleo, Seguridad Social y otras administraciones con competencia en ámbito laboral, así como aseguradoras.

    3.1.- Gestión de canal de denuncias interno, vinculado necesariamente al área jurídica, y en base a la normativa vigente:

    - Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
    - Estatuto de los Trabajadores.
    - Ley Orgánica 3/2007 para la igualdad efectiva entre mujeres y hombres
    - Estatutos de la Entidad

4. **Área Logística (Técnica y Mantenimiento)**: Estudio, informe, asesoramiento y propuesta de carácter técnico, así como la coordinación, dirección y mantenimiento de las instalaciones e infraestructuras.
    - **Fichero vinculado a la gestión Administrativa**

5. **Área de Comunicaciones**: gestión y tratamiento de las comunicaciones y contactos de la Entidad, con seguimiento de registros de entrada y salida, así como la difusión de su ámbito público, todo ello a través de cualquier medio de comunicación. Se incorpora la información a los sectores y áreas pertinentes.
    - **Fichero de Comunicaciones, Agenda de Contactos y Correo Electrónico**: generado y dedicado al control de recursos de comunicaciones y contactos.
    - **Fichero de Gestión WEB**: recoge la información incorporada a través del operativo WEB, incluidas direcciones IP.
    - **Registro de Entrada/Salida** dedicado a la gestión de recepción y envío de documentación oficial.

2.1.2.- PROCESOS DE TRATAMIENTO DE LA INFORMACIÓN

2.1.2.1.- RECOGIDA

A.- DATOS DE CARÁCTER PERSONAL: Legitimada en base a al consentimiento otorgado por el interesado para el tratamiento de sus datos personales para uno o varios fines específicos, contrato/encargo de prestación de servicios en base al objeto social de la entidad, y vinculada a las funciones definidas en su objeto social. Estando sujeta a la legislación correspondiente y a sus propios Estatutos.

A.1.- PERSONAS FÍSICAS no vinculadas contractualmente: La entidad, en principio no recoge datos de carácter personal (identificativos) de particulares, dada su funcionalidad de gestora de proyectos recoge datos, no obstante, de darse la

circunstancia de recogida, ello se realiza a través de formularios documentales y aplicación electrónica.

 En la recogida directa se informa a los usuarios de los diversos pormenores que exige la normativa, responsable del tratamiento, finalidad, plazo de tratamiento, etc., así como de la posibilidad del ejercicio de los derechos establecidos por la normativa vigente en materia de protección de datos.

A.2.- PERSONAL LABORAL: la entidad recoge directamente los datos de su personal laboral en base a la legislación vigente en materia de empleo, informando a los trabajadores de todos los aspectos que exige la normativa.

o Dispone de un Documento de Responsabilidad en el cual se les informa de sus deberes y obligaciones en el ámbito del tratamiento de datos personales.

A.2.i.- SOLICITANTES EMPLEO: la entidad puede recoger currículum de forma directa o bien a través de convocatorias de bolsa de empleo, informando de todos los extremos que la legislación dispone y custodiándose con seguridad.

B.- DATOS PERSONALES DE CARÁCTER EMPRESARIAL O REPRESENTATIVO: Legitimada en base , contrato/encargo de prestación de servicios en base al objeto social de la entidad, y vinculada a sus funciones definidas. Estando sujeta a la legislación de fundaciones, administrativa, tributaria, transparencia y a sus propios Estatutos.

Estos datos se consideran fuera del ámbito de la protección de datos de carácter personal (Considerando 14 RGPD), dado su carácter empresarial y representativo, no obstante, se cumplen las medidas informativas, de confidencialidad, finalidad y seguridad.

2.1.2.2.- TRATAMIENTO

a.- GENERAL

- PROCESOS: el tratamiento se realiza bajo procesamiento mixto (documental e informático), con software de gestión y sistemas de archivo documental.
- CESIONES/ COMUNICACIONES: se comunican bajo necesidad de servicios y obligaciones legales. Se reseña la posible publicación en web corporativa, en base a la sujeción de la normativa de transparencia.

Se hace observar que la comunicación de datos a un Encargado de Tratamiento no constituye cesión según la normativa vigente.

b.- PERSONAL LABORAL: la entidad trata los datos del personal laboral de acuerdo con lo establecido en la legislación laboral y el estatuto de los trabajadores.

- PROCESOS: el tratamiento se realiza bajo procesamiento informático, con software de gestión específico, para control laboral, elaboración de nóminas y seguimiento de prevención de riesgos laborales, así como cuantas sean necesarias en base a la relación contractual.
- CESIONES: no se realizan cesiones, salvo aquellas que puedan estar exigidas legalmente, como puede ser la administración laboral y tributaria.
- COMUNICACIONES: los datos pueden ser comunicados a la administración pública vinculada en el ámbito laboral y fiscal, asesores, aseguradoras y

entidades de prevención de riesgos laborales, así como a entidades bancarias. Se reseña que la comunicación de datos a un Encargado de Tratamiento no constituye cesión según la normativa vigente.

c.- ENCARGADOS DE TRATAMIENTO. La entidad dispone de los contratos exigidos para el tratamiento de datos por parte de terceros, especificándose en los mismos todos los extremos que la legislación exige, especialmente los servicios vinculados, la tipología de datos afectos a tratamiento y las exigencias de seguridad.

2.1.2.3.- ALMACENAMIENTO

La información se conserva centralizada en servidores dedicados, ubicados en las instalaciones de la propia Entidad, así como copias de seguridad realizada bajo responsabilidad de encargados de tratamiento.

La información en formato documental se encuentra en archivadores en las instalaciones en zonas reservadas y de no acceso público.

2.1.2.4.- CONSERVACIÓN

Los datos son tratados mientras se mantenga la relación establecida, ya sea tanto de servicios como en el ámbito laboral.

Se señala especialmente que dada su vinculación a actividad pública los datos, bajo finalidad de transparencia, que hayan sido publicados en web corporativa, serán eliminados de dicha difusión una vez concluida su necesidad.

Tras la finalización de la relación:

- De haber consentimiento o no haber oposición podrán ser usados para comunicaciones de la Entidad.
- De no haber consentimiento o haberse registrado oposición, serán conservados bloqueados con el fin de hacer frente a las posibles responsabilidades legales y administrativas, el plazo que la legislación competente (administrativa, fiscal y laboral) disponga.

2.2.- ÁMBITO ESPECÍFICO ENS

El Esquema Nacional de Seguridad, de aplicación a todo el Sector Público, así como a los proveedores que colaboran con la Administración, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. *(Art. 1, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.)*

En base a lo anterior será ámbito de incidencia del ENS los medios electrónicos dispuesto por la FIMABIS para la gestión de su objeto social, concretamente

- ✓ Direcciones de correo electrónico corporativos

Así como sus sistemas de gestión y almacenamiento vinculados

3. OBJETIVOS Y MISIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

FIMABIS ha establecido un marco de gestión de la seguridad de la información según lo establecido por la normativa y legislación vinculada, así como la norma ISO 27001 de seguridad de gestión de los sistemas de información, reconociendo como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de las normas que constituyen el marco de referencia es sentar las bases sobre las cuales el personal, colaboradores y clientes, así como terceras partes interesadas de FIMABIS, puedan acceder y prestar los servicios en un entorno de gestión seguro, anticipándose la organización a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege la información de las amenazas a la que ésta puede verse sometida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos y servicios de FIMABIS.

El marco de gestión de seguridad de la información abarca igualmente la protección de datos de carácter personal y tiene en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD, así como lo contemplado en la legislación de carácter nacional en dicha materia, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos de Carácter Personal y garantía de los Derechos Digitales

La gestión de la seguridad de la información garantiza el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de éstos.

Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Implementar el valor de la Seguridad de la Información en el conjunto de la organización, contribuyendo con la gestión de la seguridad a cumplir la misión y objetivos establecidos por FIMABIS.

2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales, normativos y de nuestros clientes y partes interesadas relativos a la seguridad de la información que resulten de aplicación como consecuencia de la actividad desarrollada, especialmente los relativos a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

3. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, estableciendo un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos, y a la monitorización continuada de nuestra actividad.

4. Proteger los activos de la información de FIMABIS y los sistemas de información que la soportan de todas las amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad en la prestación de nuestros servicios y la seguridad de la información en las vertientes de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

5. Definir como marco de gestión de la seguridad y el compromiso de mejora continua, utilizando como referencia la normativa y legislación en seguridad y licitud del tratamiento de la información.

6. Garantizar que todas y cada una de las personas que componen la organización de FIMABIS contribuyen a la protección de la Seguridad de la Información, aportando los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados, asegurando que el personal conozca y siga las normativas de seguridad de FIMABIS y asumiendo la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

7. Extender nuestro compromiso con la seguridad de la información a nuestros clientes, colaboradores y proveedores, así como a terceras partes interesadas.

Esta Política de Seguridad asegura un compromiso manifiesto de la Dirección de FIMABIS, para su difusión, consolidación y cumplimiento.

Fundamentos de esta Política

El objetivo último de la seguridad de la información es garantizar que una organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

Seguridad como proceso integral.

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se promoverá la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Gestión de la seguridad basada en los riesgos.

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, con dichos riesgos a niveles aceptables, y se realizará mediante la aplicación de medidas de seguridad de manera proporcionada a la naturaleza de la información tratada y de los servicios a prestar.

Prevención, detección, respuesta y conservación.

La seguridad del sistema contempla medidas que implementen los aspectos de prevención, detección y respuesta ante incidentes de seguridad, y de conservación de la información y servicios en caso de que el incidente se produzca.

Existencia de líneas de defensa.

FIMABIS, implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Vigilancia continua y reevaluación periódica.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

FIMABIS, implementa controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Las medidas de seguridad se evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Diferenciación de responsabilidades.

FIMABIS, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge más adelante en este documento.

En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento.

4. ALCANCE

La presente Política de Seguridad de la Información del SGSI es aplicable y de obligado cumplimiento a quienes tengan acceso los recursos que hayan sido identificados como “activos de información” de FIMABIS dentro del alcance establecido del sistema de gestión de la seguridad, a sus recursos y a los procesos afectados por el ENS, RGPD y

LOPDGDD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Dichos requisitos de protección afectan a toda la información en soporte electrónico o soporte papel y a los sistemas de información propiedad de la organización o gestionados para la misma.

5. MARCO LEGAL Y NORMATIVO

- ✓ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- ✓ Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- ✓ Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- ✓ Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ✓ Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- ✓ Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- ✓ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- ✓ Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ✓ Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- ✓ Ley 39/2022, de 30 de diciembre, del Deporte.

Y las normas:

- ✓ UNE-ISO/IEC 27001:2023 Seguridad de la Información, ciberseguridad y protección de la privacidad. SGSI. Requisitos.
- ✓ UNE-ISO/IEC 27002:2023 Seguridad de la Información, ciberseguridad y protección de la privacidad. Control de Seguridad de la Información.

El Esquema Nacional de Seguridad amplía su información y requisitos mediante las guías publicadas por el Centro Criptológico Nacional, guías que deben ser aplicadas según conciernan.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de FIMABIS en el ámbito de la prestación de sus servicios y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados de sus clientes empresas, entidades y administraciones públicas en el ejercicio de su actividad y competencias.

5. AUTORIDAD SOBRE LA POLÍTICA Y REVISIÓN

El Comité de Seguridad tiene la autoridad para verificar el cumplimiento de la presente Política de Seguridad, la responsabilidad de hacer cumplir las directrices generales y actuaciones correspondientes contenidas en el mismo y la independencia para plantear acciones correctivas y preventivas necesarias para cumplir los objetivos del plan de tratamiento de riesgos y la mejora continua de la seguridad de la información.

Es responsabilidad de todas las personas y departamentos implicados en los procesos o servicios incluidos en el alcance, el obligado cumplimiento de la presente Política de Seguridad. Para conseguir este propósito es necesaria la implicación y participación de todo el personal de FIMABIS.

El Comité de Seguridad de la Información es responsable de la presente Política de Seguridad y deberá realizar la revisión de este documento con al menos una periodicidad anual para valorar la vigencia del presente texto o la necesidad de su actualización en base a nuevos riesgos aparecidos o nuevas necesidades de garantizar la seguridad de la información.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad de la Información.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de FIMABIS son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, acordes con las funciones desempeñadas.

Para una mejor respuesta ante incidentes de seguridad, FIMABIS mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen los objetivos propuestos en la presente política de seguridad requieren del establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad de la información.

La dirección de FIMABIS, asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información, determinando en cada caso los motivos y el plazo de vigencia. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen con relación a cada responsabilidad en Seguridad de la Información.

La gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, definidas y documentadas que se describe en los párrafos siguientes. A tal fin la entidad dispone de un Protocolo de Buenas Prácticas a disposición y suministrado a todo el personal.

6.1. ROLES Y RESPONSABILIDADES

6.1.1. Usuarios/as

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de FIMABIS, se considerará un usuario. Los/las usuarios/as son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos y documentales de FIMABIS. El/la usuario/a es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los/las usuarios/as tienen la obligación de:

- Proteger y custodiar la información de FIMABIS, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de las políticas, normas, procedimientos y medidas de seguridad aplicables.

Los/las usuarios/as que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con FIMABIS, y con la legislación vigente y aplicable.

6.1.2. Responsable de la Información

Le corresponde la potestad de establecer los requisitos de la información en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de la información:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.

Dicha potestad se ejercitará de acuerdo con la Gerencia de FIMABIS, quien determinará los requisitos de seguridad aplicables a la información bajo su responsabilidad y su nivel correspondiente.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

Responsable del tratamiento

De acuerdo con lo especificado en el RGPD y la LOPDGDD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Este rol, que recae sobre FIMABIS, representada por la figura del Gerente.

6.1.2. Responsable de la Seguridad y servicio

El Responsable de la Seguridad de la Información tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por el responsable de la información y de los servicios:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad y de la Norma UNE-ISO/IEC 27001.
- Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse, necesarias para la protección de la información manejada y los servicios prestados y verificar que las establecidas son adecuadas en todo momento.
- Informar a los Responsables de la Información y de los Servicios de las incidencias de seguridad.
- Reportar el estado de la seguridad al Comité de Seguridad de la Información.
- Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
- Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa así como de la seguridad física y lógica de los recursos.
- De acuerdo con el Comité de Seguridad, promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.
- Mantener la documentación del SGSI organizada y actualizada, gestionando los mecanismos de acceso y aprobación de esta.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Responsable de los servicios/ departamentos

Son los roles que deben establecer los requisitos de seguridad aplicables a los servicios bajo su responsabilidad. Este rol estará ostentado por cada uno de los responsables de los departamentos de FIMABIS. Ostentarán las siguientes responsabilidades específicas:

- Determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

Se destaca el Responsable de RRHH, que cumplirá la función de implicar a todo el personal de la organización en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y colaboradores y de la capacitación continua de los mismos en materia de seguridad.

6.1.3. Responsable y administrador de los sistemas

El responsable de los sistemas de información será el encargado de aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la Seguridad. Este rol lo asumirá el Responsable TIC de FIMABIS que será designado por la Gerencia, pudiendo ser un Encargado de Tratamiento, asumiendo las siguientes responsabilidades específicas:

- ✓ 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.
- ✓ Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- ✓ Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- ✓ Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- ✓ Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- ✓ Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- ✓ Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- ✓ Elaborar en colaboración con el Responsable de Seguridad, la documentación de Procedimientos Operativos Instrucciones Técnicas.

- ✓ Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

Como administrador del sistema.

Sus funciones más significativas son las siguientes:

- ✓ La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- ✓ La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- ✓ La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- ✓ La aplicación de los Procedimientos Operativos de Seguridad.
- ✓ Aplicar los cambios de configuración del sistema de información.
- ✓ Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- ✓ Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- ✓ Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- ✓ Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- ✓ Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- ✓ Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.1.4.- Asesor jurídico y Compliance

Su función primordial es la de garantizar la correcta y adecuada aplicación de la normativa vigente en cada una de las actuaciones realizadas por la entidad. Así mismo, como coordinador compliance se encarga de establecer estándares y procedimientos adecuados para evitar incumplimientos. Además, supervisa y controla que éstos se cumplan en toda la organización.

6.1.5. Delegado de Protección de Datos

Tiene asignadas las funciones contempladas en el art. 39 del Reglamento General de Protección de Datos. En el contexto que nos ocupa:

- ➢ Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben con relación al RGPD y otras disposiciones de protección de datos.
- ➢ Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

La designación para el desempeño de este rol se efectuará por la Dirección de FIMABIS.

6.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES

6.2.1. Junta Directiva de FIMABIS

En materia de seguridad de la información, la Gerencia de FIMABIS tiene las siguientes funciones:

- Aprobar, representada por la Dirección en el Comité de Seguridad de la Información, la Política de Seguridad de la Información de FIMABIS y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento del ENS, la ISO 27001 y el Reglamento General de protección de datos.
- Aprobar el desarrollo organizativo propuesto por el Comité de Seguridad de la Información (Comité SI).
- Nombramiento y cese de los integrantes del Comité SI.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité SI.

6.2.2. Comité de Seguridad de la Información (SI)

El Comité SI tiene las siguientes funciones:

- Elaborar y proponer la política de seguridad de la organización de FIMABIS, para su posterior aprobación por la Gerencia.
- Velar por que la seguridad de la información sea parte del proceso de planificación de FIMABIS
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Elaborar y proponer a la Gerencia el desarrollo organizativo que permita el cumplimiento del ENS, la ISO 27001, así como del Reglamento General de Protección de Datos y normativa complementaria.
- Recabar informes regulares del estado de seguridad de la información de la organización y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la Gerencia y al Comité.
- Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de los distintos departamentos.
- Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica de FIMABIS.
- Promover acciones de concienciación, formación y motivación del personal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento

de las expectativas de los departamentos, usuarios y la protección de su información.

Este comité está conformado por los siguientes roles permanentes:

- Responsable de la Información: FIMABIS
- Responsable de Seguridad y Servicio: D. JOSÉ MIGUEL GUZMÁN, GERENCIA
- Responsable de los Sistemas: D. DAVID GÓMEZ
- Asesor Jurídico y Compliance: Dª INMACULADA MENA/ Dª EVA PENA
- Delegado de Protección de Datos: D. JOSÉ MONTILLA, DPD

Según los temas tratados, podrán ser convocados a reuniones también:

- Responsable de RRHH.
- Directores/Responsables de Área.
- Responsable de Administración.

La Dirección podrá revisar los nombramientos del Comité de Seguridad de la Información cuando estime oportuno.

7. ÁMBITOS DE GESTIÓN CUBIERTOS POR LA POLITICA

7.1. ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- ✓ Al menos una vez al año (mediante revisión y aprobación formal).
- ✓ Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y herramientas al efecto de la Agencia Española de Protección de Datos. El nivel de riesgo máximo aceptable se establecerá en base a la metodología elegida.

El nivel máximo de riesgo aceptable se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen.

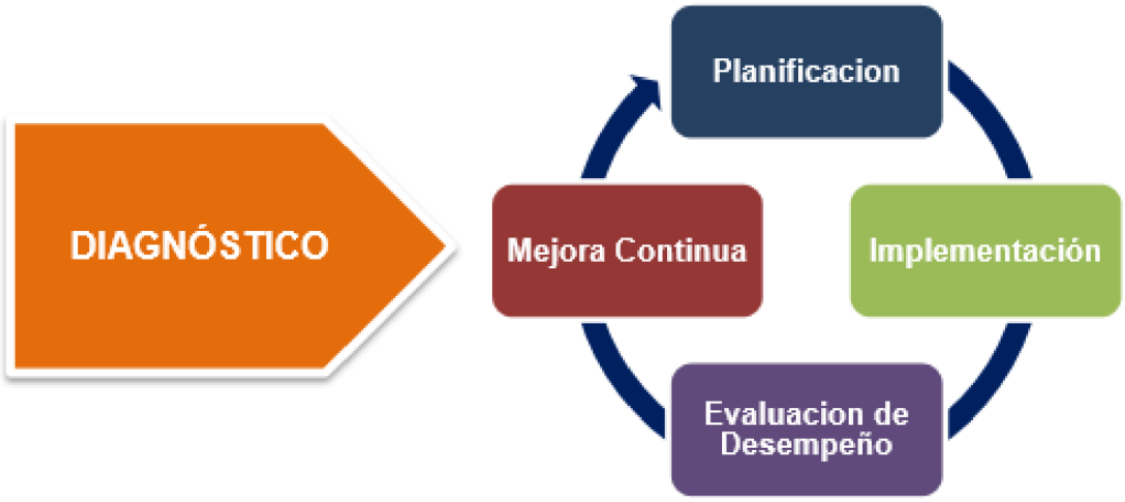
Si el tratamiento de los riesgos establece necesarias medidas adicionales a las definidas para el RGPD, LOPDGDD, ENS o la ISO 27001, incluidas las medidas que pudieran derivarse del tratamiento de datos personales, se añadirán éstas a las descritas en la normativa.

7.2. PLANIFICACIÓN y METODOLOGÍA

En este ámbito se contemplan las directrices relacionadas con la planificación de la seguridad dentro de FIMABIS, tanto en lo referente al análisis y gestión de los riesgos de seguridad de la información como en lo relativo a la planificación general de la seguridad de los sistemas de información de FIMABIS.

FIMABIS establece su estrategia de protección de los sistemas de información en la constitución de múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, física y lógica, dispuestas de tal forma que, si una de ellas falla, la seguridad del sistema en su conjunto no sea comprometida. Además, los sistemas de información se diseñan de forma que garanticen la seguridad por defecto, considerando expresamente la seguridad en su arquitectura.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.



Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos

Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas

Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones

7.3. CONTROL DE ACCESOS

Este dominio cubre las directrices de FIMABIS relacionadas con el control de acceso a los sistemas de información, tanto en lo referente a la gestión de usuarios como en lo relativo a la gestión de permisos y mecanismos de autenticación. En términos generales, estas directrices establecen que el acceso a los sistemas de información debe estar controlado, monitorizado y limitado exclusivamente a los usuarios, procesos,

dispositivos y sistemas de información que estén debidamente autorizados, de forma que se restrinja el acceso a las funciones permitidas.

Los identificadores de usuario/a utilizados en los sistemas de información se asignan de forma unívoca, de modo que cada identificador está asociado a un único usuario o proceso. Existe un procedimiento formal para gestionar las altas, bajas y modificaciones de usuario/a.

Los/las usuarios/as de FIMABIS cuentan con soluciones de control de acceso a los sistemas de información que permiten limitar el acceso a la información, siendo los responsables de los servicios los que determinan dicha autorización. Estas autorizaciones se otorgan de acuerdo con los principios generales de mínimo privilegio, necesidad de conocer y capacidad de autorizar.

Los mecanismos de autenticación utilizados se encuentran definidos en el procedimiento de gestión de usuarios/as.

7.4. EXPLOTACIÓN

Dentro de este ámbito se recogen todas las directrices establecidas por FIMABIS en relación con las medidas de seguridad a considerar durante la explotación de los sistemas de información. Aquí se contempla tanto la configuración segura de los sistemas como su mantenimiento, de modo que se gestione la seguridad a lo largo de todo el ciclo de vida de los sistemas de información, ya sea informático y/o documental.

Todos los sistemas de información de FIMABIS son configurados inicialmente de forma segura, de modo que proporcionan exclusivamente las funcionalidades mínimas necesarias, se limita el acceso a ellas y se configuran de forma que su uso natural sea sencillo y seguro por defecto.

La instalación de cualquier componente físico o lógico de un sistema de información requiere una autorización formal previa. Se mantiene un inventario actualizado de todos los componentes de los sistemas de información instalados y sus responsables. Una vez puestos en producción existe una sistemática de mantenimiento de los sistemas de información que estipula las tareas de mantenimiento a llevar a cabo, de acuerdo con las directrices de los fabricantes, y que regula la gestión de las actualizaciones de seguridad en función de la vulnerabilidad y el riesgo asociados.

Los incidentes de seguridad que se producen, y en particular los asociados con malware, son clasificados, registrados y tratados diligentemente, utilizándose dichos registros para la optimización de las medidas de seguridad implantadas.

FIMABIS, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- ✓ Mecanismos para responder eficazmente a los incidentes de seguridad.
- ✓ Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- ✓ Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias.
- ✓ Para garantizar la disponibilidad de los servicios, FIMABIS, S.L dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Los usuarios disponen de canales establecidos para informar de forma inmediata de cualquier incidente o anomalía detectada.

7.5. SERVICIOS EXTERNOS

En este ámbito se contemplan las directrices definidas por FIMABIS con relación a la utilización de recursos externos a la organización, estableciendo como premisa general que FIMABIS sigue siendo en todo momento responsable de los riesgos en que se incurra por el uso de los servicios externos utilizados, de forma que la organización debe adoptar las medidas necesarias para poder ejercer dicha responsabilidad y mantener el control de las funciones delegadas.

Se hará partícipes a los terceros de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

FIMABIS exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

FIMABIS regula contractualmente la utilización de recursos externos a la organización, estableciendo en dichos contratos las características del servicio, las responsabilidades de cada parte, la calidad mínima exigible y las consecuencias del incumplimiento del contrato. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está 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 de la Información 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, así como del responsable del tratamiento previsto en el RGPD y LOPDGDD, antes de seguir adelante.

Con relación al seguimiento y gestión diaria de los servicios externos utilizados, FIMABIS lleva a cabo un seguimiento periódico del cumplimiento de las obligaciones pactadas contractualmente, estableciendo con cada proveedor una sistemática específica para la coordinación del servicio, la monitorización de su calidad y la resolución de las desviaciones y conflictos que puedan surgir.

Cuando FIMABIS preste servicios a organismos o maneje información de organismos o AAPP, se les hará partícipe de esta Política de Seguridad de la Información y se establecerán canales para el reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

7.6. CONTINUIDAD

Dentro de este ámbito se recogen las directrices relacionadas con la continuidad de los servicios prestados por los sistemas de información de FIMABIS. Así, se establece como garantía básica que todos los sistemas de información disponen de copias de seguridad actualizadas periódicamente, y que la organización ha establecido los mecanismos necesarios para garantizar la continuidad de sus servicios informáticos y de comunicaciones en caso de pérdida de las infraestructuras originales. Estas copias de

seguridad están en línea con el análisis de impacto de los servicios informáticos y de comunicaciones de FIMABIS, que identifica los requisitos de disponibilidad de cada servicio.

7.7. MONITORIZACIÓN

Este dominio cubre las directrices de FIMABIS relacionadas con la monitorización tanto de los propios sistemas de información como del uso que los/las usuarios/as hacen de ellos. En términos generales, estas directrices establecen la obligatoriedad de registrar la actividad de los/las usuarios/as durante su uso de los sistemas de información, con el nivel de detalle necesario para identificar actividades indebidas o no autorizadas salvaguardando al mismo tiempo los derechos de los/las usuarios/as.

FIMABIS tiene establecidas soluciones de monitorización de los sistemas que permiten supervisar su comportamiento y detectar/prevenir la intrusión en ellos. Así mismo, la organización cuenta con indicadores que permiten medir el grado de implantación, eficacia y eficiencia de las medidas de seguridad establecidas, tanto técnicas como organizativas y operativas.

FIMABIS ha habilitado registros de la actividad de los/las usuarios/as reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los/las afectados/as, y de acuerdo con la normativa sobre protección de datos personales y demás disposiciones que resulten de aplicación.

7.8. INSTALACIONES E INFRAESTRUCTURAS

En este ámbito se contemplan las directrices definidas por FIMABIS con relación a la protección de las instalaciones y las infraestructuras físicas, articuladas mediante el control de acceso físico y el acondicionamiento y protección frente a contingencias ambientales. En términos generales, estas directrices se resumen en que los sistemas de información se instalan en salas específicas y separadas, que deben permanecer cerradas, dotadas de mecanismos de control de acceso, como llaves o claves, cuya distribución debe estar controlada.

Los servidores y el equipamiento de red principal están instalados en los CPDs de FIMABIS, pudiendo disponer de Encargados de Tratamiento. En todo caso, el acceso a las ubicaciones está controlado y todos los accesos a estas salas se registran. Todos los visitantes (personal no autorizado por defecto, tanto propio de FIMABIS como ajeno) son identificados previamente a dicho acceso.

Los CPDs y sistemas de archivo, de FIMABIS y/o el Encargado de Tratamiento vinculado, están equipados con sistemas de control y acondicionamiento que velan por el buen funcionamiento del equipamiento albergado en ellos, siguiendo lo dispuesto en las normativas y procedimientos de control de acceso físico y lógico.

7.9. PERSONAL, CONCIENCIACIÓN Y FORMACIÓN

Este ámbito contiene las directrices de FIMABIS en materia de gestión del personal, y contempla todos los aspectos relacionados con la formación y capacitación, la concienciación y difusión y la gestión de sus deberes y obligaciones. FIMABIS establece la obligación de que todo el personal afectado conozca sus deberes y obligaciones en materia de seguridad, y los respete en el ejercicio de sus funciones. Para ello, FIMABIS se compromete a regular formalmente estos deberes y obligaciones y a formar al personal sobre ellos, de modo que la seguridad de los sistemas de información sea

respetada, aplicada y supervisada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

FIMABIS establece las funciones y obligaciones que en materia de seguridad son aplicables a cada puesto de trabajo, identificando las condiciones de confidencialidad a cumplir y las medidas disciplinarias asociadas en caso de incumplimiento.

FIMABIS también establece los requisitos que debe cumplir todo el personal que sin pertenecer a la organización está relacionado con ella y afectado por esta Política, como es el personal perteneciente a empresas subcontratadas u otro tipo de colaboradores o socios.

Así mismo, FIMABIS tiene un programa de formación y concienciación que garantiza que periódicamente todo el personal recibe la información necesaria para saber cómo realizar su trabajo de manera segura y cómo debe participar en la gestión de la seguridad de los sistemas de información y los incidentes que puedan producirse, con el fin de que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad.

7.10. EQUIPAMIENTO Y RESPONSABILIDADES DEL USUARIO

Dentro de este ámbito se recogen las directrices relacionadas con la gestión segura del equipamiento y material puesto a disposición de los/las usuarios/as, en relación tanto a las obligaciones de FIMABIS al respecto como a las responsabilidades que los/las usuarios/as deben asumir durante su uso.

El personal debe velar porque el puesto de trabajo esté despejado, de modo que no haya más material sobre su mesa que el requerido para la actividad que se esté realizando en cada momento. Ese material se deberá guardar en un lugar cerrado, como armarios o cajones, cuando no se esté utilizando.

Los equipos portátiles, al tener la consideración de entornos inseguros, deberán contar con medidas de seguridad adicionales. Por una parte, estos equipos estarán equipados con un firewall personal, que limite su visibilidad y controle el acceso al equipo cuando se conecte a redes públicas. Por otra se habilitarán normativas para controlar los equipos portátiles que posee la organización, su responsable y su ubicación y para reportar incidentes relacionados con pérdidas o sustracciones de dichos equipos. Así mismo, sus usuarios también deberán limitar la información que contienen estos equipos, evitando, en la medida de lo posible, que contengan claves de acceso remoto a la red de FIMABIS.

7.11. COMUNICACIONES

Este dominio cubre las directrices de FIMABIS relacionadas con la gestión de las redes de comunicaciones, principalmente de cara a su interconexión con redes ajenas, que en general tendrán la consideración de entornos inseguros. En general, estas directrices se resumen en la obligatoriedad de proteger el perímetro de la red, en particular si se conectan a redes públicas, y de controlar los puntos de interconexión, aplicando medidas de seguridad en función de los riesgos derivados de dicha interconexión.

FIMABIS y/o el Encargado de Tratamiento vinculado, según lo dispuesto en la arquitectura de seguridad, dispone de cortafuegos que separan las redes internas del exterior, de modo que cualquier tráfico entre redes internas y externas debe atravesarlos, estando configurados de forma que sólo se permiten los flujos de datos previamente autorizados, y monitorizando los que sean necesarios en base al riesgo.

7.12. SOPORTES DE INFORMACIÓN

En este ámbito se contemplan las directrices definidas por FIMABIS con relación a la protección de los soportes de información, entendidos como todo el equipamiento móvil electrónico y no electrónico sobre el que se almacena información de forma estática (papel, pen-drives, CDs, DVDs, cintas, discos, entorno de nube, etc.), que tendrán la consideración de entornos inseguros. Estas directrices se pueden resumir en tener la precaución de adoptar las medidas de seguridad pertinentes para proteger la información almacenada en estos dispositivos durante su uso y transporte, y garantizar su conservación y recuperabilidad a largo plazo.

Todo el personal de FIMABIS debe aplicar la debida diligencia y control a los soportes de información que permanezcan bajo su responsabilidad, garantizando que se cumplen las medidas de control de acceso físico y/o lógico aplicables y que se respetan unas exigencias ambientales mínimas apropiadas para su conservación.

Toda la información en soporte papel que haya sido causa o consecuencia de la información electrónica tratada por los sistemas de información deberá estar protegida con el mismo grado de seguridad que ésta, aplicando las medidas de seguridad apropiadas a la naturaleza del soporte en que se encuentren.

Los soportes de información electrónicos deberán estar etiquetados de forma que permitan identificar el nivel máximo de seguridad de la información contenida. Siempre que sea necesario su contenido deberá estar cifrado, y el responsable de sistemas deberá garantizar su control, registrando sus entradas y salidas y su eliminación segura.

7.13. APLICACIONES

Este ámbito contiene las directrices de FIMABIS en materia de desarrollo y puesta en producción de aplicaciones, que regulan los principales aspectos a considerar desde el punto de vista de la seguridad en torno a estas actividades.

En relación con la puesta en producción de aplicaciones, FIMABIS y/o Encargado de Tratamiento vinculado, disponen de un entorno aislado en el que se llevan a cabo las pruebas, realizadas con datos previamente ofuscados. Estas pruebas contienen una parte funcional y otra parte de seguridad, en la que se verifica el cumplimiento de los criterios de aceptación en materia de seguridad y que su puesta en marcha no provoca deterioros en la seguridad de otros componentes del sistema de información afectado.

7.14. INFORMACIÓN

Dentro de este ámbito se recogen las directrices de FIMABIS relacionadas con la protección de la información, relativas tanto a la protección específica de los datos de carácter personal de acuerdo con las exigencias del RGPD como a la protección general de toda la información gestionada por FIMABIS en el ejercicio de sus funciones.

FIMABIS cumple de forma escrupulosa las exigencias legales vigentes en materia de protección de datos de carácter personal, aplicando de manera global a esta información las medidas de protección preceptivas por dicha regulación, sin perjuicio de cumplir, además, otras medidas de seguridad adicionales en caso de que se considere necesario.

FIMABIS clasifica la información en virtud de su naturaleza, identificando responsables de la información de acuerdo con lo establecido en la presente Política. Los criterios de clasificación y designación de responsables están identificados en el procedimiento correspondiente, en base a los cuales estos responsables podrán modificar dicha clasificación.

Como norma general de protección de la información, FIMABIS establece la obligatoriedad de llevar a cabo copias de seguridad que permitan recuperar datos pasados. Así mismo, la organización establece la obligatoriedad de llevar a cabo procesos de limpieza de documentos, según los dispuesto en el procedimiento de borrado de metadatos.

7.15. VIGILANCIA CONTINUA

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

FIMABIS implementa controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Las medidas de seguridad se evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

8. DESARROLLO Y DESPLIEGUE DE LA POLÍTICA DE SEGURIDAD

8.1. INSTRUMENTOS DE DESARROLLO

La Política de Seguridad de la Información de FIMABIS se desarrollará por medio en una serie de documentos normativos en los que se recogerán políticas de seguridad específicas para los distintos ámbitos contemplados. Dichos documentos normativos podrán adoptar alguna de las siguientes modalidades:

- ✓ Documentación del desarrollo del SGSI (SGSI): Incluyen los aspectos generales del SGSI: Política de Seguridad, Análisis de Riesgos, Normativa, Categorización del Sistema y la Declaración de Aplicabilidad.
- ✓ Procedimientos generales (PGS): Incorporan procedimientos generales de actuación del sistema de gestión de seguridad de la información.
- ✓ Procedimientos operativos de seguridad (POS): Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.
- ✓ Instrucciones técnicas (ITS): Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas.

Todo ello se recogerá en un Documento de Seguridad y Protocolo de Buenas Prácticas.

En caso de que la normativa desarrollada afecte de manera general a los/las usuarios/as de los sistemas de información de FIMABIS, dicha afección deberá ser previamente aprobada por el Comité de Seguridad.

Las políticas, normativas y regulaciones específicas que se aprueban se notifican y difunden apropiadamente a todos/as los/las afectados/as.

La normativa general de utilización recursos y sistemas de información estará disponible en la intranet de FIMABIS a disposición de todo el personal de la entidad que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones, que incluyan datos de carácter personal.

8.2. SANCIONES PREVISTAS EN CASO DE INCUMPLIMIENTO

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores y el Convenio Colectivo vigente en FIMABIS en cada momento.

ANEXOS

A.1.- Constitución Comité Seguridad

A.2.- Declaración de Aplicabilidad

B.1.- Gestión acreditativa ENS

B.2.- Gestión acreditativa L.O.P.D.G.D.D.