SGSI01 – Política de Seguridad

Clasificación de la Información:

Nivel del Documento	Documento cumplimiento ENS
Nombre del Fichero	SGSI01 – Política de Seguridad
Tipo	RESTRINGIDO
Ámbito de Difusión	Todos los empleados y colaboradores externos
Responsable	Responsable de Seguridad de la Información

CONTROL DE MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Versión preliminar del documento.	0.1	19/11/2019
Primera Versión del documento	0.2	20/11/2020
Segunda Versión del documento	0.3	03/03/2021

Contenido

1. Introducción

La presente Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del **Real Decreto 951/2015, de 23 de octubre**, de modificación del **Real Decreto 3/2010,** de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (**ENS**), en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

Esta Política de Seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN), centro adscrito al Centro Nacional de Inteligencia (CNI).

La **Ley 40/2015**, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados y recoge el Esquema Nacional de Seguridad en su artículo 156.

Mientras que la **Ley 39/2015**, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos/usuarios y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La adaptación al ENS implica que la **Fundació Lluís Alcanyís** y su personal deben aplicar las medidas mínimas de seguridad exigidas por el propio ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades de gestión de la Fundació Lluís Alcanyís deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y los costes asociados deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Las unidades de gestión de la Fundació Lluís Alcanyís deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2. La seguridad como proceso integral

La seguridad de la información es el resultado de un proceso que depende de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en el tratamiento. Quienes participen en cualquier fase del tratamiento deberán responder, en la medida de sus responsabilidades, de la seguridad y buen uso de la información. De manera especial, deberán colaborar en la prevención, detección y control de los riesgos derivados de actuaciones negligentes, ignorancia de las normas, fallos técnicos, de organización o de coordinación, o instrucciones inadecuadas.

Un comité formado por los distintos agentes con responsabilidades específicas en materia de seguridad se encargará de proporcionar los canales de participación adecuados que hagan efectiva la colaboración mencionada en el párrafo anterior. Del mismo modo, se ocupará de mantener permanentemente informados, a todos los destinatarios de esta política, del propósito y contenido de la misma, así como de los documentos que la desarrollan y de los canales de participación habilitados.

El proceso de gestión de la seguridad de la información deberá estar sometido a monitorización, control y mejora continuos para confirmar su eficiencia ante la constante evolución de los riesgos y de los sistemas de protección.

2.1. Prevención

La Fundació Lluís Alcanyís debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

La Fundació Lluís Alcanyís debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la Fundació Lluís Alcanyís.

2.4. Recuperación

Para restaurar la disponibilidad de los servicios, se deberán contar con planes de contingencia de los sistemas TIC que incluyan la recuperación de la información.

3. Misión

La Fundación tiene por objeto promover, cooperar y fomentar el desarrollo de actividades docentes teóricas y prácticas y de investigación de las enseñanzas que se imparten en la Universitat de València, a fin de obtener una completa formación de su alumnado adecuada a las necesidades sociales de cada momento, la realización de actividades enfocadas a la formación del profesorado, actividades de formación continuada y formación de personas en situación de desocupación, la transferencia de resultados de la investigación y de transferencia del conocimiento, así como colaborar con la Universitat de València en la gestión de actividades relacionadas con la prestación de servicios socio-sanitarios.

4. Alcance

La Fundació Lluís Alcanyís aplicará la presente Política de Seguridad sobre aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

De forma concreta, atendida la misión de la Fundació Lluís Alcanyís definida en el punto 3, la presente Política de Seguridad es aplicable sobre los siguientes Sistemas de Información TIC y Servicios que los conforman:

- [SIS-AP] Sistema de Atencion al paciente
    - [S-APODO] Atención al paciente Odontología
    - [S-APPOD] Atención al paciente Podología
    - [S-APNUT] Atención al paciente Cunaff
    - [S-APOPT] Atención al paciente Optometría
    - [S-APPSI] Atención al paciente Psicologia
    - [S-APLOG] Atención al paciente Logopedia

- [SIS-FOR] Sistema de Formación
    - [S-WEB] Página web
    - [S-QYS] Quejas y sugerencias
    - [S-FOR] Formación
    - [S-MAR] Marketing y RRSS
    - [S-GAL] Gestion Alumnos

- [SIS-RRHH] Sistema de Gestión de Recursos Humanos
    - [S-RRHH] Gestión de RRHH

- [SIS-ADM] Sistema de Gestión Administrativa
    - [S-FEL] Facturación electrónica
    - [S-PTR] Portal Transparencia
    - [S-ALE] Alquiler Espacios
    - [S-PCN] Perfil del Contratante
    - [S-COF] Servicio de contabilidad y Facturación

La organización desestima la aplicación de la presente Política de Seguridad sobre aquellos sistemas de información no reflejados en este apartado.

5. Marco normativo complementario

En el desarrollo e implementación de esta política se tendrán en cuenta los Estatutos de la Fundació Lluís Alcanyís, así como sus normativas de desarrollo relacionadas con los objetivos del mismo.

6. Organización de la seguridad

De acuerdo con el ENS se estructura un organigrama de seguridad de la Fundació Lluís Alcanyís en 3 niveles:

- Nivel 1:
  - Comité de Gestión y Coordinación de la Seguridad de la Información.
  - Responsable de la Información.
  - Responsable del Servicio.
  - Delegado de Protección de Datos.

- Nivel 2:
  - Responsable de la Seguridad de la Información.

- Nivel 3:
  - Responsables de los Sistemas de Información.

La especificación de requisitos de seguridad (nivel 1) corresponde a los responsables de la información y de los servicios. La operación (nivel 3) corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad (nivel 2) y al técnico de seguridad (nivel 3).

Por encima de todos ellos existe el Comité de Coordinación y Gestión de la Seguridad (nivel 1). Este Comité de Seguridad puede asumir también la responsabilidad de la Información y de los Servicios.

6.1. Comité de gestión y coordinación de la seguridad de la información

El Comité de Gestión y Coordinación de la Seguridad de la Información, en adelante **Comité de Seguridad de la Información**, coordina la seguridad de la información a nivel de organización.

De acuerdo con el ENS las funciones indicadas que corresponden al Comité de Seguridad son:

- Elaborar (y revisar periódicamente) la Política de Seguridad de la información para que sea aprobada por la Dirección de la Fundació Lluís Alcanyís.
- Aprobar y divulgar los procedimientos de seguridad.
- Promover la mejora continua de la gestión de la seguridad de la información de la entidad.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Evaluar los principales riesgos residuales asumidos por la Fundació Lluís Alcanyís y recomendar posibles actuaciones respecto a ellos.
- Evaluar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas y evaluar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad de acuerdo con los recursos disponibles.
- 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, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la Política de Seguridad.

El Comité de Seguridad de la Información estará formado por:

- Dirección, que presidirá el comité.
- Responsable de la Información.
- Responsable del Servicio (El rol de Responsable de los Servicios será asumido por el Comité de Seguridad)
- Responsable de Seguridad de la Información, que actuará como secretario del comité.
- Responsable de los Sistemas

El Comité de Seguridad no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad se asesorará en los temas sobre los que tenga que decidir o emitir una opinión.

6.2. Responsable de la Información

El Responsable de la Información establecerá los requisitos sobre la información proporcionada por medios electrónicos a través de los servicios de la Fundació Lluís Alcanyís y, por tanto, tendrá la última palabra a la hora de decidir el tipo de información accesible y el uso que se le pueda dar, en virtud de la reglamentación vigente y de las buenas prácticas en materia de Protección de Datos. Le corresponden las siguientes funciones:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y los responsables de los sistemas en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

El responsable de la información será Dirección.

6.3. Responsable de los Servicios

El Responsable de los Servicios establecerá los requisitos de seguridad aplicables a los servicios proporcionados por la Fundació Lluís Alcanyís a través de medios electrónicos y, en este sentido, tendrá como funciones:

- Establecimiento de los requisitos de los servicios TIC en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y los responsables de los sistemas donde se englobe el servicio para el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

El rol de Responsable de los Servicios será asumido por el Comité de Seguridad.

6.4. Responsable de Seguridad de la Información

Las funciones del Responsable de Seguridad de la Fundació Lluís Alcanyís son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.
- Planificar las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de la Seguridad de la Información dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de monitorización y auditoría de los estados de seguridad de los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el Comité de Seguridad incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por los Responsables de los Sistemas cuando en virtud del contenido no requiera la aprobación del Comité de Seguridad.

- Proponer la redacción de aquella normativa de seguridad de la Fundació Lluís Alcanyís que considere necesario formalizar.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo a la puesta en marcha de un nuevo servicio vinculado al ENS.

6.5. Responsables de los Sistemas

Se designará un único responsable para todos los sistemas de información definidos en el apartado de Alcance de este documento.

Dentro de sus áreas de actuación y en el marco es esta Política de Seguridad, los Responsables de los Sistemas llevarán a cabo las siguientes funciones:

- Velar por el correcto funcionamiento del Sistema durante todo su ciclo de vida, de sus especificaciones e instalación, incorporando los requisitos de seguridad necesarios para la operativa en el sistema.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Proponer al Responsable de Seguridad los cambios que afecten a la seguridad del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar los requisitos de la configuración autorizada del hardware y software a utilizar en el Sistema, en lo que afecte a su seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema que afecte a la seguridad y disponibilidad del servicio.
- Llevar a cabo el preceptivo proceso de revisión periódica del análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las actuaciones que afecten a la Política de Seguridad de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

6.6. Delegado de Protección de Datos

Dentro de la protección de datos, el DPO se encargará de asesorar y supervisar, entre otras, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgos de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

El rol del DPO será asumido por el DPO de la Universitat de València.

6.7. Procedimientos de designación

El desempeño de las responsabilidades definidas en esta Política de Seguridad vendrá determinado por el acceso a los diferentes cargos que se han vinculado a ellas. En el caso de que desapareciese o cambiará de denominación alguno de estos cargos será competencia de la Dirección de Fundació Lluís Alcanyís asignar el nuevo puesto al que quedará vinculada la figura.

7. Datos de carácter personal

La Fundació Lluís Alcanyís realiza tratamientos en los que hace uso de datos de carácter personal sometidos a lo dispuesto por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Las políticas de seguridad aplicables a los tratamientos se rigen por las medidas de seguridad implantadas de acuerdo al Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En el RAT (Registro de Actividades del Tratamiento) se indexan los distintos tratamientos de datos afectados por la normativa.

Todos los sistemas de información de la Fundació Lluís Alcanyís se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

7.1. Política de privacidad de datos de carácter personal

Esta Política de protección de datos de carácter personal será de aplicación para todos los empleados o contratista.

Las personas que actúen como representantes de Fundació Lluís Alcanyís en sociedades y entidades observarán las previsiones de esta Política de protección de datos de carácter personal y promoverán, en la medida de lo posible, la aplicación de sus principios.

El Delegado de Protección de Datos será responsable de velar por que la regulación, prácticas y procedimientos internos sean conformes con la regulación en materia de protección de datos que resulte aplicable en cada caso y deberá difundir e informar de los desarrollos y novedades normativas que se produzcan en este ámbito.

7.2. Principios del tratamiento de datos de carácter personal

Los principios por los que se rige la Política de protección de datos de carácter personal son los siguientes:

a) Principios Generales:

La Fundació Lluís Alcanyís cumplirá escrupulosamente con la legislación en materia de protección de datos de carácter personal en cada país.

Además, velará por el cumplimiento del principio de calidad de los datos, que se concreta en que solo se recogerán y se tratarán datos personales cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se recojan o traten, que deberán ser concretas y legítimas, salvo en los casos en que la legislación aplicable establezca otra cosa.

La Fundació Lluís Alcanyís procurará que los datos personales recabados sean veraces y exactos. Además, promoverá que los principios recogidos en esta Política de protección de datos de carácter personal sean tenidos en cuenta:

(i) en el diseño e implementación de todos los procedimientos establecidos por la misma organización,

(ii) en los productos y servicios ofrecidos por estas,

(iii) en todos los contratos y obligaciones que formalicen o asuman y

(iv) en la implantación de cuantos sistemas y plataformas permitan el acceso de empleados o terceros y/o la recogida o tratamiento de datos de carácter personal.

b) Principios Relativos a la Recogida y al Tratamiento de los Datos:

En la medida en que así lo exija la legislación aplicable, en los procesos de recogida y tratamiento de datos de carácter personal, se informará de modo expreso, preciso e inequívoco, al menos, acerca de la existencia de dicho proceso, de la identidad de los responsables del tratamiento de los datos y de la finalidad de la recogida de los datos de conformidad con la normativa aplicable y con el Sistema de Gestión de la Privacidad.

En los casos en que resulte obligatorio según la normativa aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar o tratar sus datos.

La Fundació Lluís Alcanyís no recabará ni tratará datos personales relativos a la ideología, religión, creencias, origen racial o étnico, u orientación sexual, salvo que la recogida de los referidos datos sea requerida para ofrecer un servicio específico al paciente o por la legislación aplicable, en cuyo caso serán recabados y tratados de acuerdo con lo establecido en aquella.

c) Principios en Materia de Medidas de Seguridad y Confidencialidad:

La Fundació Lluís Alcanyís diseñará, implantará, ejecutará y mantendrá todas las medidas de seguridad organizativas y técnicas que sean necesarias para garantizar que la recogida y el tratamiento de los datos se realicen cumpliendo los estándares exigidos legalmente.

d) Principios sobre las Cesiones de Datos:

Queda prohibida la compra u obtención de datos de carácter personal de fuentes ilegítimas o en aquellos casos en los que dichos datos hayan sido recabados o cedidos contraviniendo la ley o no se garantice suficientemente su legítima procedencia.

e) Principios sobre la Contratación de Encargados del Tratamiento:

Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos de carácter personal que sean responsabilidad de La Fundació Lluís Alcanyís, así como durante la vigencia de la relación contractual, la propia entidad, verificará que el prestador de servicios reúne las garantías necesarias y cumple con las medidas de seguridad exigibles en cada jurisdicción.

f) Transferencias Internacionales de Datos:

Todo tratamiento de datos de carácter personal sujeto a normativa de la Unión Europea que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen.

g) Principios sobre los Derechos de los Afectados:

La Fundació Lluís Alcanyís permitirá que los afectados puedan ejercitar los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, que sean de aplicación en cada jurisdicción, estableciendo a tal efecto los procedimientos internos que resulten necesarios y oportunos, los cuales deberán satisfacer, al menos, los requisitos legales aplicables en cada caso.

8. Gestión de riesgos

Todos los sistemas sujetos a esta Política de Seguridad realizarán un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados.

9. Desarrollo de la Política de Seguridad

Esta Política se desarrolla por medio de una **Normativa de Seguridad** que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el disco UV habilitado para este fin. Para consultarla, se podrá solicitar al Responsable de Seguridad.

10. Obligaciones del personal

Todos los miembros de Fundació Lluís Alcanyís tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias de La Fundació Lluís Alcanyís.

Todos los trabajadores de la Fundació Lluís Alcanyís bajo el alcance del ENS atenderán a una acción de concienciación en materia de seguridad TIC, Se establecerá un programa de acciones en concienciación continua para informar a todos los miembros de la Fundació Lluís Alcanyís.

Se realizará una acción de concienciación durante los dos años siguientes a la aprobación de esta Política de Seguridad y de manera continuada para el personal de nueva incorporación.

En su caso, si se requiere formación específica para el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su trabajo.

11. Terceras partes

Cuando la Fundació Lluís Alcanyís preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. Para ello, se establecerán canales para informar y coordinar los respectivos Comités de Seguridad del ENS y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Fundació Lluís Alcanyís utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, debiéndose incorporar a los contratos y encomiendas de la Fundació Lluís Alcanyís. Con ello, el proveedor deberá garantizar que su personal está adecuadamente formado en materia de seguridad de acuerdo con los requerimientos de la Fundació Lluís Alcanyís.

12. Entrada en vigor

La presente Política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación por la Dirección de la Fundació Lluís Alcanyís y hasta que sea reemplazada por una nueva Política.

Se dispondrá de los medios para publicar, dar a conocer y facilitar el cumplimiento de esta política y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad. Asimismo, habilitará canales de participación que permitan, a los destinatarios de esta política y de los documentos complementarios, participar en su revisión y mejora.

APROBADO:
Fecha: 03/03/2021
Firma:
JOAN MARIA| MANSANET| MANSANET Firmado digitalmente por JOAN MARIA|MANSANET| MANSANET Fecha: 2021.03.03 10:10:24 +01'00'