1010 – Política de Seguridad de la Información (ENS)

Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain)

(+34) 973 282 300 · info@lleida.net

Control Documental

Fecha	Versión	Modificaciones	Autor
19/07/2023	1.0	Creación	Eva Pané
26/05/2025	1.1	Revisión	Eva Pané

Lista de distribución

Departamentos
Lleida.net

Clasificación y estatus del documento

Clasificación del documento	Uso interno

Estatus del documento	Aprobado

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

1 Índice

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

1 Introducción

1.1 Objetivo

El presente documento, establece la Política de Seguridad de la Información de Lleidanetworks Serveis Telemàtics, S.A. ("LLEIDA.NET" o "Lleida.net"), que es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

En consonancia con el Artículo 1 del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* (ENS)[1], esta política establece los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Serán aplicados por LLEIDA.NET para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en la prestación de los servicios contemplados en el alcance.

Esta política complementa y desarrolla la *1001- Política de Seguridad* elaborada en el marco del SGSI de acuerdo con los requisitos de la norma ISO 27001.

2 Alcance

La presente política se refiere a los sistemas de información que dan soporte a los procesos de negocio de los siguientes servicios y las áreas de soporte asociadas (alta dirección, recursos humanos, seguridad física, IT y compliance:

> SMS, SMS certificado, Contrato SMS, Email certificado, Recepción certificada, Factura certificada, Contrato email certificado, Tools, Click & Sign, Openum y Validador Universal Certificado de Firmas Digitales (USVC)

En relación con el documento de determinación de la categoría vigente.

Asimismo, la presente política aplica a todos los empleados y colaboradores de Lleida.net sin excepciones, así como todas las terceras partes identificadas en el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI). En concordancia con el artículo 13 del ENS, esta política establece que la seguridad de la información compromete a todos los miembros y colaboradores de la organización. Mediante esta política de seguridad se identifican unos claros responsables de velar por su cumplimiento y que sea conocida por todos los miembros y colaboradores de la organización.

[1] Ver referencia al *Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad* en el punto *2.2 Marco Legal.*

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

2.1 Distribución y revisión

En el documento "*1006 – Inventario documental*" se muestran la lista de distribución y la responsabilidad de revisión y aprobación de este documento, así como el estado de actualización y documentos a los que se referencia.

2.2 Objetivos y misión de la organización

Como la Primera Operadora Certificadora, nuestra misión consiste en aportar seguridad, confianza, eficacia y rentabilidad a las comunicaciones electrónicas de empresas, administraciones públicas y particulares, influyendo directamente en la mejora de sus resultados. Innovamos para satisfacer las necesidades de nuestros clientes, conseguir una rentabilidad creciente y sostenible para nuestros accionistas y facilitar el desarrollo profesional de nuestros empleados.

Nuestro objetivo es ser la operadora líder a nivel internacional en el mercado de la certificación de comunicaciones electrónicas, prestando servicios que sean reconocidos como estándares. Queremos aportar a la sociedad nuevas formas de comunicarse que mejoren y faciliten las relaciones entre las personas, convirtiendo procesos de comunicación tradicionales en servicios de valor acordes a las nuevas tecnologías.

Esta misión y objetivo se desarrollan en la *1001–Política de Seguridad* y en el *1002-Alcance del SGSI.*

Para conseguirlos, Lleida.net ha establecido como valores primordiales de la organización:

- ✓ **Liderazgo**

  Compromiso, profesionalidad, eficiencia y trabajo en equipo.

- ✓ **Confianza**

  De los clientes y de la sociedad, basada en un servicio y una atención de máxima calidad con las mayores garantías de seguridad y eficacia.

- ✓ **Accesibilidad**

  En el uso de servicios adaptados a la totalidad de la sociedad sin barreras físicas, sensoriales o de cualquier otro tipo.

- ✓ **Sostenibilidad y responsabilidad**

  De la empresa con un crecimiento responsable, velando por las condiciones de los trabajadores, fomentando su desarrollo personal y profesional a la vez que se facilita la conciliación de la vida laboral y familiar.

2.3 Marco legal

El marco legal que aplica a Lleida.net en el desarrollo de su actividad está determinado en el apartado *6. Marco normativo* de este documento y desarrollado en el *2015-Reglamento de cumplimiento legal regulatorio y contractual.*

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 ·
info@lleida.net

Entre otras, establece la necesidad de conformidad con el Esquema Nacional de Seguridad en cumplimiento del Artículo 2.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad que establece que:

> 3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

3 Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Lleida.net recogidas en el Sistema Integrado de Gestión y adecuadas a los controles necesarios según la *1011-Categorización y Declaración de Aplicabilidad ENS Lleida.*

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que Lleida.net ha puesto en marcha un Sistema de Gestión de la Seguridad de la Información, según el cual se aplican las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), y se realiza un seguimiento continuo de los niveles de prestación de servicios, se siguen y analizan las vulnerabilidades reportadas, y se prepara una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

El conjunto de áreas y departamentos de Lleida.net debe contemplar la seguridad TIC como 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 las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Esta Política de Seguridad de la Información se ha desarrollado mediante diversas normativas y reglamentos documentados en el SGSI que afrontan diversos aspectos específicos.

Asimismo, se ha elaborado el Handbook que está 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.

Estas normativas y reglamentos están disponibles según el procedimiento *3001-Gestión del repositorio de documentación* y la 1007-*Política de Comunicación*, y forma parte de la formación obligatoria para todos los empleados de Lleida.net.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

4 Categorización de los sistemas de información

En aplicación de los criterios establecidos en el artículo 40 del ENS, la categoría de los sistemas de información dentro del alcance de esta política, en materia de seguridad, modulará el equilibrio entre la importancia de la información que manejan, los servicios que prestan y el esfuerzo de seguridad requerido, en función de los riesgos a los que están expuesto, bajo el criterio del principio de proporcionalidad.

La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que pudiera afectar a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, tal como queda recogido en el documento *1011-Categorización y Declaración de Aplicabilidad ENS Lleida*.

Atendiendo a lo establecido en el Anexo I del ENS, los fundamentos para la valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para:

a) el logro de sus objetivos

b) la protección de sus activos

c) el cumplimiento de sus obligaciones de servicio y contractuales

d) el respeto de la legalidad vigente

e) el respeto a los derechos de las personas.

Para determinar el nivel requerido para cada dimensión de seguridad se toma como referencia la identificación y valoración de los principales activos de servicios y de información determinada en el *4301.01 - Análisis de riesgos* y que es relativa a la importancia para el negocio. Para realizar esta valoración de activos respecto a las diferentes dimensiones de seguridad se tienen en cuenta los criterios de clasificación de la información establecidos en el documento *2007-Reglamento de clasificación y tratamiento de la información*.

En atención a las facultades determinadas en el artículo 41 del ENS, corresponderá al responsable de cada información o servicio efectuar las valoraciones aquí mencionadas, y al responsable de cada sistema la determinación de la categoría de este.

5 Principios básicos

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad de la información, trazabilidad de los servicios y datos, uso previsto y valor de la información y los servicios.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Tal como establece el Artículo 5 del ENS, el objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Reevaluación periódica.
f) Diferenciación de responsabilidades.

Es importante remarcar que, tal como establece el artículo 8 del ENS, la seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta la organización.

5.1 La seguridad como un proceso integral

Tal como se refleja en el artículo 6 del ENS, la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La política de seguridad de la información estará regida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

El conjunto de áreas y departamentos de Lleida.net deben contemplar la seguridad de la información como 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 las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos dentro del alcance de esta política.

5.2 Gestión de la seguridad basada en los riesgos

En consonancia con los principios establecidos en los artículos 6 y 14 del ENS, la apreciación, análisis y tratamiento de los riesgos serán parte esencial de la gestión de la seguridad y deberán mantenerse permanentemente actualizados

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos apreciados.

Este análisis se realizará de siguiendo la *1004-Metodologia de identificación, análisis y gestión de riesgos* y se revisará regularmente, al menos una vez al año, o cuando:

a) Cambien los activos de información manejados;

b) cambien los servicios prestados;

c) ocurra un incidente grave de seguridad;

d) se reporten vulnerabilidades graves.

5.3 Prevención

Las diferentes áreas y departamentos sujetos al alcance de esta política deben 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 han implementado las medidas mínimas de seguridad determinadas por el ENS, así como los controles adicionales identificados a través de una evaluación de amenazas y riesgos.

Tal como se indica en el artículo 8 del ENS, las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Para garantizar el cumplimiento de la política, se han establecido los siguientes requisitos:

- 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.
- Monitorización continua del desempeño de las medidas de seguridad y de la operación de los sistemas

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

5.4 Existencia de líneas de defensa

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS que implementan una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falle, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

c) Minimizar el impacto final sobre el mismo.

Estas líneas de defensa estarán constituidas por medidas de naturaleza organizativa, física y lógica.

5.5 Vigilancia continua y detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios o la presencia de ciberincidentes, y actuar en consecuencia según el principio de vigilancia continua, establecido en el Artículo 10 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.

En la correspondiente documentación de *3004-Procedimiento SOC* se describe el proceso y políticas para supervisar y monitorizar los sistemas de modo que se pueda prevenir su degradación y asegurar la disponibilidad de capacidad suficiente.

5.6 Respuesta

Las medidas de detección estarán acompañadas de medidas de respuesta, de forma que los incidentes de seguridad se gestionan en tiempo oportuno.

El *2014-Reglamento de gestión de incidentes* determina que mediante los adecuados procedimientos operativos:

- Se han establecido mecanismos para responder eficazmente a los incidentes de seguridad.
- Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en las diferentes áreas de la empresa o terceras partes involucradas.
- Se han establecido protocolos para el intercambio de información con las partes interesadas relacionadas con el incidente.

En el *3028-Procedimiento de Gestión de Incidentes* se detalla los pasos a seguir para la gestión de incidentes.

5.7 Recuperación

Las medidas de recuperación permitirán la restauración de la información y los servicios que pudieran haberse visto afectados por incidentes disruptivos, de forma que se pueda hacer frente a las situaciones en las que estos incidentes afecten los activos habituales de tratamiento o a la integridad de la información.

Se ha elaborado el *2019-Plan de continuidad de negocio (BCP)* que contemplan el desarrollo de procedimientos de recuperación para cada uno de los riesgos de disrupción identificados que permita recuperar las actividades críticas de acuerdo con los objetivos tiempos de recuperación

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

(RTO) y punto de recuperación de los datos (RPO) establecidos según el *3026-BIA (Análisis del impacto sobre el negocio)*.

Dichos procedimientos de recuperación están documentados en el *3015-Procedimiento de reinicio y recuperación de los sistemas (DRP)*.

Asimismo, se contempla la realización de pruebas y ensayos para verificar la viabilidad y adecuación de los procedimientos de recuperación mediante los planes de prueba documentados según los correspondientes planes de continuidad.

5.8 Conservación

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Para ello, se identificarán los principales activos de información y se determinarán los requisitos de conservación y retención, que servirá como punto de partida para establecer las políticas de copias de seguridad necesarias.

La implementación de estas políticas de copias de seguridad debe permitir asegurar los supuestos de inalterabilidad de la información y limitación de acceso según el principio de mínimo privilegio.

5.9 Reevaluación periódica

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se revisarán, reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Esta revisión y reevaluación periódica se llevará a cabo dentro del marco de gestión de riesgos y mejora continua del Sistema de Gestión de la Seguridad de la información.

5.10 Diferenciación de responsabilidades

De acuerdo con el principio de diferenciación de responsabilidades establecido en el artículo 11 del ENS, Lleida.net establece funciones y responsabilidades de forma que la seguridad de la información se gestione como función diferenciada

Las políticas que aplican para la definición de estas funciones y responsabilidades están cubiertas en el apartado *7. Organización de la Seguridad* de este documento

6 Marco normativo

La legislación aplicable y cuyo cumplimiento se requiere para cumplir los objetivos de seguridad de la información está documentada en el *2015-Reglamento de cumplimiento legal regulatorio y contractual.*

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

En particular para esta política se establece el marco normativo estipulado para el Esquema Nacional de Seguridad, así como las instrucciones técnicas de seguridad y guías de seguridad que le son de aplicación al sistema (Art 29).

En lo que hace referencia específicamente al Esquema Nacional de Seguridad, se contempla:

- *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*
- Instrucciones técnicas de seguridad de obligado cumplimiento, según lo previsto en el artículo 29 del Real Decreto 3/2010
    - Informe del estado de la seguridad
    - Conformidad con el Esquema Nacional de Seguridad
    - Auditoría de la seguridad de los sistemas de información
    - Notificación de incidentes de seguridad

  El contenido de estas instrucciones técnicas será de obligado cumplimiento en cuanto sus disposiciones se apliquen a una entidad del sector privado no sujeta a las obligaciones establecidas por la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*.
- Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, se tendrán como referencia las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800 que elabora y difunde el CCN.

Asimismo, se contempla dentro del marco normativa el complimiento voluntario de estándares en seguridad de la información tal como la ISO 27001.

7 Organización de la Seguridad

7.1 Comités: Funciones y responsabilidades

Se ha constituido el Comité de Gestión de la Seguridad de la Información de acuerdo con las políticas establecido en el documento *1003 - Organización de la seguridad de la información*. En él se detallan su composición, sus funciones y responsabilidades.

El Comité de Gestión de la Seguridad de la Información reportará a la Dirección de Lleida.net en todos aquellos aspectos que por su impacto pueden ser relevante para la dirección de la organización.

7.2 Roles: Funciones y responsabilidades

En el documento *1003 - Organización de la seguridad de la información* se identifican los cargos en seguridad de la información en cumplimiento del artículo 10 del ENS, así como las atribuciones, funciones y responsabilidades de cada uno de los cargos, así como el procedimiento para su designación y renovación.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

En Lleida.net se han determinado los siguientes cargos, con referencia a los puestos de trabajo definidos en el organigrama de la organización ya las responsabilidades y funciones determinadas en el documento *1003 - Organización de la seguridad de la información:*

- **Responsable de Seguridad de la información**
- **Responsable del Sistema**
- **Responsable de la información**
- **Responsable del Servicio**
- **Administrador de Seguridad**

La persona designada será aquella que en cada momento ocupe el puesto de trabajo referenciado.

En cumplimiento de lo establecido en el artículo 13 del ENS, Lleida.net designa a la persona Responsable de Seguridad como POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, a fin de que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

7.3 Procedimiento para la designación y renovación de roles

Los roles y funciones de seguridad serán los determinados en esta Política, y su designación y renovación estará formalizada con la aprobación de esta política.

En caso de que exista alguna variación en las personas designadas para cada uno de los cargos relacionados, la persona substituta automáticamente asumirá las funciones y responsabilidades inherentes a los roles de seguridad que le son propios, quedando dicha designación formalizada en una posterior reunión del Comité de Gestión de la Seguridad de la Información.

7.4 Mecanismo de coordinación y resolución de conflictos

En el documento *1003 - Organización de la seguridad de la información s*e establece el Comité de Gestión de la Seguridad de la Información como órgano para la coordinación y resolución colegiada de conflictos.

En el caso de que no se llegará a ningún acuerdo en el marco de este Comité, corresponderá a la Alta Dirección de Lleida.net ejercer la función de arbitraje y tomar las decisiones oportunas.

7.5 Política de Seguridad de la Información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será revisada por los miembros permanentes del Comité de Seguridad de la Información, aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 ·
info@lleida.net

7.6 Gestión de la documentación

En el *3001-Gestión del repositorio de documentación* se determinan las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Asimismo, se indica cuál es el criterio para la calificación de la documentación, el procedimiento para su calificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse

8 Requisitos de seguridad de la información

Esta Política de Seguridad contempla todos los requisitos mínimos de seguridad determinados en el artículo 12 del ENS.

8.1 Organización e implantación del proceso de seguridad

Tal como se establece en el apartado Alcance de esta política, la seguridad compromete a todos los miembros de Lleida.net.

Según se detalla en el apartado *7. Organización de la Seguridad*, se identifican unos claros responsables de velar por el cumplimiento de esta Política de Seguridad de la Información, y que deberá conocida por todos los miembros de Lleida.net.

8.2 Análisis y gestión de riesgos

Este análisis y gestión se llevará a cabo tal como se dispone en el apartado *5.2. Gestión de la seguridad basada en los riesgos* de esta política.

8.3 Gestión del personal

Todos los miembros de Lleida.net tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normativa y reglamentos de seguridad determinada en el SGSI, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

En el *2012-Reglamento de seguridad en RRHH* se establecen los procedimientos necesarios para garantizar una correcta gestión de los Recursos Humanos (RRHH) de Lleida.net en cuanto a la seguridad de la información.

Se prestará la máxima atención a 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 fuentes de riesgo para la seguridad.

Todos los miembros de Lleida.net atenderán a la formación obligatoria en materia de Seguridad de la Información, y participarán en programas de concienciación continua.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en este.

El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema queda concretado en normativa de seguridad de la información que todos los empleados deben conocer.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad

8.4 Profesionalidad

La seguridad de los sistemas de Lleida.net estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y operación.

La cualificación del personal se determina en los requisitos de cada puesto de trabajo según se especifica en las descripciones de puesto de trabajo correspondientes.

El personal de Lleida.net está comprometido en cumplir y hacer cumplir las políticas de seguridad de la información. Esta obligación está contemplada en la normativa que deben cumplir todos los empleados.

Lleida.net exigirá, de manera objetiva y no discriminatoria, que las terceras partes que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

8.5 Terceras partes

Cuando Lleida.net preste servicios a otros organismos o maneje información de otros organismos, si así lo requieren, se les hará partícipes de esta Política de Seguridad de la Información.

Cuando Lleida.net utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que aplique a los servicios proporcionados por los proveedores y que está establecida en el *2016-Reglamento de gestión de terceros*. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

En cualquier caso, los proveedores de servicios de terceros deberán proporcionar garantías de seguridad de la información suficientes y adecuadas a los servicios prestados. En el caso particular de aquellos servicios que se presten dentro del marco del alcance de la certificación ENS, se exigirá que los proveedores presten sus servicios de conformidad con los requisitos del ENS que les apliquen.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Cuando algún aspecto de estas políticas 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 antes de seguir adelante.

8.6 Autorización y control de los accesos

Se han definido diferentes procedimientos donde se han establecido los procesos formales de autorizaciones que cubren todos los elementos de los sistemas de información.

a) Utilización de instalaciones, habituales y alternativas.

b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.

c) Entrada de aplicaciones en producción.

d) Establecimiento de enlaces de comunicaciones con otros sistemas.

e) Utilización de medios de comunicación, habituales y alternativos.

f) Utilización de soportes de información.

g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

h) Utilización de servicios de terceros, bajo contrato o convenio.

El acceso a los sistemas de información de Lleida.net está controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

La política de control de accesos a los sistemas de información está documentada en según el *2009-Reglamento de seguridad en el control de acceso*. Adicionalmente, se han establecido diversos procedimientos tal como el *3006-Procedimiento para el alta y baja de usuarios*, el *3007-Procedimiento para la entrega de credenciales y login* y el *3008-Procedimiento para la gestión de permisos de administración.*

8.7 Protección de las instalaciones

El recinto de Lleida.net está protegido mediante diversos sistemas de vigilancia y un sistema de control de acceso basado en anillos de seguridad, con niveles de restricción incrementales.

La infraestructura de sistemas se ha instalado en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas están cerradas y disponen de un control de acceso específico.

Asimismo, cuando se utilizan infraestructuras de terceros para alojar los sistemas que prestan los servicios, estos terceros deberán proporcionar garantías conformes se cumplen los requisitos de seguridad establecidos por las políticas de Lleida.net y son conformes a los requisitos del ENS aplicables.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Se dispone del *3009-Procedimiento de seguridad física* que contiene las instrucciones para la gestión de la seguridad física en las distintas instalaciones de Lleida.net.

8.8 Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad de las TIC que vayan a ser empleados por Lleida.net se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en lo relativo a profesionalidad y cualificación del personal y niveles de gestión.

La adquisición de productos y contratación de servicios de seguridad se regirá por lo establecido en los documentos *2016-Reglamento de gestión de terceros* y *3017 – Procedimiento de gestión de terceros*.

8.9 Mínimo privilegio

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto y se apliquen políticas de mínimo privilegio basadas estrictamente en la “necesidad de conocer”:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

8.10 Integridad y actualización del sistema.

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema, de acuerdo con los diferentes procedimientos establecidos al efecto.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, con relación a 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.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

8.11 Protección de información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

A este respecto se deberán aplicar las medidas de protección acordes a la clasificación de la información contenidas en estos soportes según se define en el *2007-Reglamento de clasificación y tratamiento de la información.*

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

8.12 Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas.

En todo caso, de acuerdo con el *3020-Procedimiento de seguridad red* se analizarán los riesgos derivados de la interconexión de los sistemas, a través de redes, con otros sistemas, y se controlará su punto de unión, aplicándose mecanismos basados en controles criptográficos para asegurar la autenticidad de los extremos de la comunicación y la confidencialidad e integridad de la información según se define en el *2002-Seguridad de los sistemas.*

8.13 Registro de actividad y detección de código dañino

Para aquellos sistemas y aplicaciones sea necesario registrar la actividad de los usuarios, este registro se realizará con la finalidad exclusiva de cumplir los requisitos normativos que sean de aplicación, o para garantizar la trazabilidad de los servicios si así lo determina la evaluación de riesgos.

Este registro se realizará con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales.

Se registrarán las actividades de los usuarios, 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.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Al objeto de preservar la seguridad de los sistemas de información, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, Lleida.net podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

8.14 Incidentes de seguridad

Lleida.net debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes.

En el *3028-Procedimiento de Gestión de incidentes* se establecen el proceso de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.

Estos procedimientos cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

Este registro se empleará para la mejora continua de la seguridad del sistema.

Asimismo, se establece un sistema de detección y reacción frente a código dañino.

8.15 Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo según se establece en los requisitos de 2019-*Plan de continuidad de negocio (BCP).*

Asimismo, se han elaborado los correspondientes planes de continuidad documentados en el *3015-Procedimiento de reinicio y recuperación de los sistemas (DRP)* para garantizar la disponibilidad de los servicios críticos a partir de los requisitos y riesgos identificados para las actividades incluidas en el alcance.

8.16 Protección de los datos de carácter personal

Lleida.net trata datos de carácter personal de acuerdo con los requisitos establecidos por el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

8.17 Ciclo de vida de servicios y sistemas.

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

8.18 Mejora continua del proceso de seguridad

El Sistema de Gestión de la Seguridad de la Información será actualizado y mejorado de forma continua en el marco del Sistema Integrado de Gestión de Lleida.net tal como establece en el *2018-Reglamento de control de la seguridad de la información y mejora continua.*

Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de la seguridad de la información de acuerdo con la norma ISO 27001:2022.

9 Cumplimiento de requisitos mínimos

En referencia al artículo 27 del ENS, para dar cumplimiento a los requisitos mínimos establecidos, se aplicarán las medidas de seguridad adecuadas teniendo en cuenta:

- La identificación y valoración de los activos que constituyen el sistema, recogido en el *2004-Reglamento de los activos de la información* y documentación derivada.
- La categoría del sistema, determinada como **ALTA** en el documento *1011-Categorización y Declaración de Aplicabilidad ENS Lleida.*
- Las decisiones que se adopten para gestionar los riesgos identificados documentadas en el plan de tratamiento de riesgos.
- El tratamiento de datos personales de acuerdo con lo establecido por la legislación vigente en materia de protección de datos personales.
- La selección de las medidas de seguridad de acuerdo con la categoría del sistema y las dimensiones de seguridad relevantes y según se relacionan en el documento *1011-Categorización y Declaración de Aplicabilidad ENS Lleida.*
- La aplicación de medidas compensatorias cuando se pueda justificar que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en el ENS.
- Las instrucciones técnicas de seguridad y guías de seguridad publicadas por el Centro Criptológico Nacional en desarrollo del artículo 29 del ENS.

10 Auditoría de Seguridad

Los sistemas de información dentro del alcance de esta política serán objeto de una auditoría externa regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

Esta auditoría se realizará en función de la categoría del sistema, determinada en el documento *1011-Categorización y Declaración de Aplicabilidad ENS Lleida.*

El resultado de cada auditoría se recogerá en un informe que deberá ser analizado por el Responsable de Seguridad, quien presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

Adicionalmente, dentro del marco de la mejora continua del proceso de seguridad se establece:

- Realización de auditorías internas de cumplimiento anuales, ya sea en base a los requisitos del ENS o cualquier otra norma de aplicación.
- Realización de auditorías técnicas regulares para la identificación de posibles vulnerabilidades y la verificación de la eficacia las medidas técnicas implantadas.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

11 Referencias

Documentación interna:

- Información documentada del SGSI
- *1002- Alcance SGSI*
- *1003-Organización de la seguridad de la información*
- *1004- Metodología de identificación, análisis y gestión de riesgos*
- *1011-Categorización y Declaración de Aplicabilidad ENS*
- *Handbook*
- *2004- Reglamento de los activos de la información*
- *2007-Reglamento de clasificación y tratamiento de la información*
- *2009-Reglamento de seguridad en el control de acceso*
- *2012-Reglamento de seguridad en RRHH*
- *2014-Reglamento de gestión de incidentes*
- *2015-Reglamento de cumplimiento legal regulatorio y contractual*
- *2016-Reglamento de gestión de terceros*
- *2018-Reglamento de control de la seguridad de la información y mejora continua*
- *2019-Plan de continuidad de negocio (BCP)*
- *3001- Gestión del repositorio de documentación*

Documentación externa:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).
- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements.

Lleida.net · Parc Agrobiotech · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net