LIMIT

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

# CONTROL DOCUMENTACIÓN

## Descripción del documento

Definición de la política de seguridad de Límit Tecnologies

## Histórico de versiones

| VERSIÓN | RESPONSABLE | DATA | DESCRIPCIÓN |
|---|---|---|---|
| 1.0 | Límit Tecnologies | 21/06/2023 | Versión original |
| 1.1 | Límit Tecnologies | 26/06/2023 | |
| | | | |
| | | | |

# ÍNDEX

# 1. INTRODUCCIÓN

La Política de Seguridad de la Información (en adelante, "Política") persigue la adopción de un conjunto de directrices destinadas a preservar, proteger y consolidar la seguridad de los servicios y los activos de información con el objetivo de mejorar la calidad de los servicios que Límit Tecnologies presta, así como:

Proporcionar un marco de control para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficiente y eficaz en todas aquellas cuestiones relacionadas con los sistemas proporcionados.

En segundo lugar, garantizar la implantación de medidas y mecanismos de seguridad apropiados para proteger los servicios prestados, los sistemas de información y la información procesada, almacenada la confidencialidad, integridad, disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, así como la autenticidad y trazabilidad de la información.

En tercer lugar, asegurar que se cumpla la normativa vigente en materia de seguridad.

Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.

Prevenir ante incidentes de seguridad de la información, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.

Impulsar y fomentar la formación, la concienciación y el cumplimiento de las obligaciones en materia de seguridad de la información del personal al servicio de la organización, a fin de garantizar el conocimiento de las políticas y las normativas aprobadas y de las prácticas recomendadas.

Establecer los objetivos y metas enfocadas hacia la evaluación del desempeño en materia de seguridad de la información, así como a la mejora continua en nuestras actividades, reguladas en el Sistema de Gestión que desarrolla esta política.

## 1.1. OBJETIVO

El objetivo principal de la presente Política es definir los principios y las medidas básicas para la gestión de la seguridad de la información.

LIMIT, consciente de que la seguridad de la información relativa a nuestros clientes es un recurso crítico, ha establecido un Sistema de Gestión de la Seguridad de la Información de acuerdo con los requisitos de la norma ISO/IEC 27001:2022 y del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad* (en adelante, "ENS") para garantizar la continuidad de los sistemas de información, minimizar los riesgos y asegurar el cumplimiento de los objetivos fijados. Depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) alcanzar los objetivos asumiendo su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas deben ser administrados con diligencia, tomando medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información tratada o los servicios prestados.

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.

Los sistemas TIC deben estar protegidos contra amenazas con potencial para afectar a la confidencialidad, integridad, disponibilidad, 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva ante los incidentes de seguridad para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, así como de los datos que tratan, 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, reacción y recuperación).

## 1.2. ALCANCE

Esta política se aplica a todos los sistemas TIC de la organización y a todos los miembros de dicha organización, implicados en una relación contractual para la prestación de servicios o prevención de soluciones en las entidades del sector público.

El alcance viene determinado por los sistemas de información y los servicios de desarrollo, diseño, implantación, provisión, soporte y mantenimiento de soluciones digitales, según la declaración de aplicabilidad vigente.

## 1.3. VIGENCIA

La aprobación de la versión 1.0 o posteriores de este documento expresa el respaldo del Comité de Seguridad de la organización al contenido del mismo. Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento.

En el caso de conflicto con otras normas o procedimientos de seguridad vigentes, será la opción más restrictiva la que prevalezca.

## 1.4. REVISIÓN Y EVALUACIÓN.

El presente documento será revisado por parte del Comité de Seguridad el cual propondrá las actualizaciones necesarias de la política de seguridad de la información para asegurar que se cumpla la legalidad vigente.

## 1.5. RESPONSABLES DE SU APLICACIÓN.

Es responsabilidad del Comité de seguridad de la información publicar y dar máxima difusión al contenido de este documento, así como dotar de los medios necesarios para garantizar su cumplimiento.

## 1.6. REFERENCIAS.

Para la confección de la actual norma se han tomado como base las siguientes referencias:

- UNE ISO/IEC 27002:2013 (Código de buenas prácticas para la Gestión de la Seguridad de la Información).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (de aquí en adelante, "LOPDGDD").
- 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 (de aquí en adelante, "RGPD").
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Reglamento (UE) Nª910/2014 del Parlamento Europeo y del Consejo, de 23 de Julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (de aquí en adelante, "LSSI")
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

- 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.
- ISO 22301:2012 (Seguridad de la Sociedad: Sistemas de Continuidad del Negocio).

# 2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## 2.1. ESTRUCTURA ORGANIZATIVA Y ROLES DE SEGURIDAD

La Dirección General de Límit Tecnologies, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito los objetivos de negocio, se compromete gestionar las funciones y responsabilidades de los trabajadores de la organización, así como facilitar los recursos adecuados para cumplir con el ENS y el RGPD en materia de seguridad de la información y protección de los datos personales. Asimismo, cumplir con los controles de la ISO 27001. Los directivos son también responsables de dar a conocer las normas de seguridad a los trabajadores de la organización y difundir el buen uso de los sistemas.

La estructura organizativa para gestionar la seguridad de la información de Límit se compone del Comité de Seguridad de la Información, Responsable de Seguridad y el Responsable de Sistemas.

## 2.2. COMITÉ DE GESTIÓN Y COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El comité para la gestión y coordinación de la seguridad o Comité de Seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

Los miembros del Comité son:

- Responsable de la Información.
- Responsable de los Servicios.
- Responsable de la Seguridad.
- Responsable del Sistema.

- Dirección Empresa (Socios-Administradores).

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

La organización de la Seguridad de la información se desarrolla en el documento complementario a esta Política de Organización de la Seguridad.

El Comité tendrá las siguientes funciones:

a) Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, con el fin de asegurar que las iniciativas en esta materia sean establecidas.
b) Elaborar la estrategia en materia de seguridad de la información estableciendo las principales directrices y responsabilidades que garanticen la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de la información y de los servicios, y alinear las actividades de seguridad con la misión y los objetivos de la organización.
c) Aprobar las medidas necesarias para aplicar y cumplir las disposiciones establecidas en la presente política de seguridad de la información.
d) Hacer el seguimiento general del estado de la seguridad de la información en la organización.
e) Aprobar y coordinar todos los proyectos de mejora o cambio sobre la seguridad de la información en aplicaciones, sistemas, activos y recursos de la organización, incluidos los planes de mejora de la seguridad.
f) Fomentar la creación y el uso de servicios horizontales que reduzcan duplicidades y apoyen un homogéneo funcionamiento de todos los sistemas de información.
g) Monitorizar los principales riesgos y recomendar posibles actuaciones al respecto.

## 2.3. ROLES Y FUNCIONES DE LOS MIEMBROS DEL COMITÉ DE SEGURIDAD

Los roles y funciones de los miembros de seguridad de la información son:

| Función | Deberes y responsabilidades |
|---|---|
| **Responsable de la información (RINFO)** | ▪ Tomar las decisiones relativas a la información tratada |
| **Responsable de los servicios (RSER)** | ▪ Coordinar la implantación del sistema<br>▪ Mejorar el sistema de forma continua |
| **Responsable de la seguridad (RSEG o CISO)** | ▪ Determinar la idoneidad de las medidas técnicas.<br>▪ Proporcionar la mejor tecnología para el servicio.<br>▪ Monitorear, documentar y analizar incidentes de seguridad. |
| **Responsable del sistema (RSIS)** | ▪ Coordinar la implantación del sistema<br>▪ Mejorar el sistema de forma continua |
| **Dirección** | ▪ Proporcionar los recursos necesarios para el sistema<br>▪ Liderar el sistema |

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades.

### 2.4. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa definida para la gestión de la seguridad de la información, lo resolverá la Dirección General; en su ausencia, prevalece la decisión del Comité para la Gestión y la Coordinación de la Seguridad de la Información.

## 3. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política serán objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos a cargo de los responsables de seguridad de la información. Este análisis se revisa regularmente:

- al menos una vez al año;
- cuando cambie la información manejada;

- cuando cambien los servicios prestados;
- cuando se identifiquen nuevos activos de información;
- 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 manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Las decisiones sobre las medidas, proyectos e iniciativas de seguridad que deban tomarse han de prever los resultados de la evaluación de los riesgos existentes en relación con la seguridad de la información sobre los sistemas utilizados. El responsable de la seguridad de la información elevará al comité correspondiente los resultados de los análisis de los riesgos.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

# 4. GESTIÓN DEL PERSONAL Y PROFESIONALIDAD

## 4.1. FORMACIÓN, CONCIENCIACIÓN Y CUMPLIMIENTO DE LAS OBLIGACIONES

LIMIT garantizará la definición y la ejecución de las acciones necesarias para concienciar y fomentar el cumplimiento de las obligaciones por parte del personal con relación a los riesgos y las amenazas relativos a la seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de la LIMIT, en particular a los de nueva incorporación.

Las personas que realicen actividades especialmente relacionadas con la seguridad de la información – en particular el personal técnico a cargo de la gestión, operación y administración de los sistemas de información – tienen que recibir las acciones formativas necesarias en materia de seguridad.

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 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 el mismo.

Todos los miembros de LIMIT atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año.

El departamento de Recursos Humanos incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

### 4.2. OBLIGACIONES DE ACATAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Todos los miembros de LIMIT tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

### 4.3. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad de la información podrá suponer el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales que correspondan.

## 5. AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de LIMIT y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

## 6. PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de LIMIT.
- Proteger el equipo de procesamiento de información crítico de LIMIT, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de la misma en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.

- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de LIMIT**.**

- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.

- Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de LIMIT: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El responsable de Gestión de la Seguridad (RSEG) [CISO], junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de LIMIT a las áreas restringidas bajo su responsabilidad. Los propietarios de información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de LIMIT cuando lo consideren apropiado.

Todo el personal de LIMIT es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

## 7. Adquisición de productos

Los diferentes departamentos 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 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.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

## 8. Seguridad por defecto

LIMIT considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

## 9. Integridad y actualización del sistema

LIMIT se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la

autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de 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.

## 10. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

LIMIT establece medidas de protección para la Seguridad de 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.

## 11. PREVENCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS

LIMIT, establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

## 12. REGISTROS DE ACTIVIDAD

LIMIT, registrará 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.

Los objetivos principales de la Gestión de incidentes son los de:

- Establecer un sistema de detección y reacción frente a código dañino.
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán 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 emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad.
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

## 13. CONTINUIDAD DE LA ACTIVIDAD

LIMIT, con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas disponen de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

## 14. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

LIMIT establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO 27001

Dirección General de LIMIT TECNOLOGIES