USO INTERNO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (ENS)

MS-07

Datos sobre la presente edición

Nº de Versión	Fecha	RESUMEN DE CAMBIOS / COMENTARIOS
1.0	28/02/2026	Creación del Documento

Consideraciones de seguridad

La presente documentación es propiedad de Lexer (en adelante Lexer o el GRUPO) y está clasificada como de USO INTERNO. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Así mismo, tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de Lexer, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme dicte la ley.

Índice

1. *Aprobación y entrada en vigor*

Texto aprobado el día 28 de febrero de 2026 por la Dirección de Lexer.

Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. *Introducción*

En Lexer el soporte de la tecnología y la evolución TIC (Tecnologías de Información y Comunicación) es una palanca crítica para alcanzar nuestros objetivos de gestión, dado nuestro enfoque a la gestión masiva. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad y confidencialidad de la información tratada, o bien la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir sus objetivos, desarrollar sus funciones / competencias y prestar los servicios para los que ha sido constituida, asegurando la calidad, disponibilidad y protección de la información, así como la prestación continuada de los servicios, mediante una actuación preventiva, la supervisión permanente de la actividad y una respuesta ágil y eficaz ante los incidentes de seguridad.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en 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 a los incidentes para garantizar la continuidad de los servicios prestados.

Lexer debe 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 donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

3. *Alcance*

La presente Política es aplicable a todos los sistemas de información que Lexer define en su alcance.

4. *Misión y objetivos de la organización*

Lexer es una compañía con un modelo de negocio único en el mercado, ofreciendo un servicio integral que abarca todas las fases de recuperación de deuda, así como un servicio especializado en real estate.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir sus objetivos, desarrollar sus funciones y competencias y prestar los servicios para los que ha sido constituida, asegurando la calidad, disponibilidad y adecuada protección de la información, así como la prestación continuada de los servicios, mediante una actuación preventiva, la supervisión permanente de la actividad y una respuesta ágil y eficaz ante los incidentes de seguridad. Nuestros servicios están soportados por los siguientes procesos:

- Extrajudicial: recuperación amistosa de deuda, se trata de contactar con el deudor al objeto de llegar a un acuerdo de pago, concretar la fecha y el modo de pago o realización de algún tipo de gestión en concreto. Dentro de este servicio se incluye la gestión amistosa asociada al sector de la automoción y depósito de vehículos.
- Judicial: inicio/gestión de procedimientos judiciales encaminados a la recuperación de la deuda a través de la vía judicial. Asesoramiento jurídico externalizado y gestión judicial en defensa de los intereses de entidades financieras. Gestión de deuda compañías automovilísticas.
- Litigación: inicio/ gestión de procedimientos judiciales orientados a la litigación bancaria en proceso específicos: gastos, tarjetas revolving, auto,…
- Procuraduría: servicio de representación procesal ante los juzgados y tribunales en defensa de los intereses de la compañía y de nuestros Clientes.
- Gestión de Activos Inmobiliarios y venta de créditos: comercialización y venta de inmuebles y créditos.

Los objetivos en materia de seguridad que Lexer pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de Lexer respecto a la seguridad de la información.
- Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.

- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. *Principios rectores de la política*

La política de seguridad de Lexer se rige por los principios básicos establecidos en el Capítulo II del Real Decreto 311/2022, los cuales constituyen el fundamento ético y profesional sobre el que se edifican todas las medidas técnicas y organizativas de la entidad:

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de Lexer, para que pueda coordinarse e integrarse con el resto de iniciativas estratégicas de la organización para formar un todo coherente y eficaz.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios para la detección y respuesta a actividades o comportamientos anómalos.
- Un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Asignación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6. *Marco normativo*

Lexer desarrolla sus actividades bajo un firme compromiso de cumplimiento con el marco legal vigente en materia de ciberseguridad, administración digital y protección de datos. Este marco se fundamenta, de manera principal pero no exhaustiva, en:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico.
- Guías CCN-STIC.

Para garantizar la vigencia de este compromiso frente a la evolución legislativa, la organización dispone de un Procedimiento de identificación de requisitos legales que define las fuentes oficiales de consulta, las responsabilidades y la sistemática de actualización. Como resultado de este proceso, se mantiene un Registro requisitos legales y normativas aplicables permanentemente actualizado.

7. *Organización de la seguridad*

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en Lexer, se designan roles de seguridad y constituye un Comité de Seguridad de la información.

7.1 Roles: funciones y responsabilidades

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

Responsable de la Información y Servicio

El Responsable de la Información y Servicio asegura la gestión, protección y disponibilidad de la información, garantizando que los servicios cumplan con los requisitos del Esquema Nacional de Seguridad (ENS) y las necesidades de la organización.

Dispone de las siguientes funciones:

- Establecer y elevar para su aprobación al Comité de Coordinación de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de Seguridad de la Información), en el marco establecido en el Anexo I del RD ENS, pudiendo recoger una propuesta del Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Regular sobre los derechos de acceso a la información.
- Aceptar los niveles de riesgo residual que afectan la información.
- Comunicar al Responsable de Seguridad cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de nueva Información a su cargo. El cual transferirá estos cambios, al Comité de Coordinación de Seguridad de la Información, en su próxima reunión.:
- Establecer y elevar para su aprobación al Comité indicado los requisitos de la seguridad aplicable en los servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recoger una propuesta del Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema (éste último rol recae en la misma persona del responsable de Seguridad).
- Dictaminar respecto a los derechos de acceso a los servicios.
- Aceptar los niveles de riesgo residuales que afecten a los servicios.

- Poner en comunicación al Responsable de Seguridad de cualquier variación respecto a los servicios de los cuales es responsable, especialmente la incorporación de nuevos Servicios a su cargo. El cual transferirá estos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

Responsable de Seguridad de la Información

Las funciones del Responsable de Seguridad corresponden con:

- Promover la formación y sensibilización en materia de seguridad de la información.
- Designar a los responsables de la ejecución del análisis de riesgos, la Declaración de Aplicabilidad, identificar las medidas de seguridad, determinar las configuraciones necesarias, preparar la documentación del sistema.
- Brindar asesoría para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o el Comité de Seguridad TIC.
- Participar en la elaboración e implementación de los planes de mejora de la seguridad y, en su caso, en los planes de continuidad, procediendo a su validación.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y que no son responsabilidad del Comité) e informar al Comité de las modificaciones que se hayan realizado a lo largo del período actual.
- Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los Servicios Electrónicos prestados por los sistemas de información
- Gestionar las revisiones externas o internas del sistema. Gestionar los procesos de certificación.
- Elevar al Comité de Coordinación de Seguridad de la Información la aprobación de cambios y otros requisitos del sistema.
- Diseñar y aplicar las políticas de protección de datos.
- Asegurar el cumplimiento del RGPD, mediante la recopilación de información, análisis y revisión de los tratamientos de datos realizados dentro de la organización, haciendo las recomendaciones que sean necesarias para garantizar su cumplimiento.

El responsable de la Seguridad podrá delegar las funciones identificadas en el punto 6, 7 y 8 en el Responsable del Sistema si así lo considera conveniente.

Responsable del Sistema

Las funciones del Responsable del Sistema se concretan en:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a la información o la prestación de servicios si tiene el conocimiento de que estos tienen graves deficiencias de seguridad.
- Asegurar que las medidas de seguridad específicas estén correctamente integradas dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Comité de Coordinación de Seguridad de la Información.
- Participar en la elaboración e implementación de planes de mejora de la seguridad y, en su caso, en planes de continuidad.
- Elaboración de procedimientos de seguridad y procedimientos técnicos de seguridad necesarios para el correcto funcionamiento de los sistemas.
- Desempeñar, cuando corresponda, las funciones del administrador de seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en el que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones otorgadas a los usuarios del sistema, en particular los privilegios otorgados, incluida la supervisión de la actividad realizada en el sistema y su correspondencia con el autorizado.
    - Aprobar los cambios en la configuración actual del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos se cumplan estrictamente.
    - Asegurar que se aplican los procedimientos aprobados para el manejo del Sistema de Información.
    - Monitorizar las instalaciones de hardware y software, sus modificaciones y mejoras para garantizar que la seguridad no se vea comprometida y que cumplan en todo momento con las autorizaciones pertinentes.
    - Supervise el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y los mecanismos de auditoría técnica.
    - Informar al oficial de seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá nombrar a los responsables de sistemas delegados que considere necesarios, quienes serán responsables en su campo de todas aquellas acciones que les delegue. Del mismo modo, también podrá delegar en otras funciones específicas las responsabilidades que se le atribuyan.

Administrador del sistema

Las funciones vinculadas a este perfil se detallan a continuación:

- Administrar y mantener los sistemas de información, servidores, redes, plataformas y componentes tecnológicos.
- Ejecutar tareas de operación diaria, mantenimiento preventivo y correctivo.
- Garantizar el funcionamiento continuo de los sistemas conforme a los niveles de servicio definidos.
- Aplicar las configuraciones de seguridad lógica y controles técnicos definidos por el Responsable de Seguridad y el Responsable del Sistema.
- Asegurar que los sistemas se mantienen configurados conforme a los principios de seguridad por defecto y mínima funcionalidad.
- Implementar medidas de hardening, control de accesos y segregación de privilegios.
- Administrar usuarios, credenciales y permisos técnicos en los sistemas bajo su responsabilidad.
- Garantizar que los accesos administrativos están controlados, registrados y limitados a lo estrictamente necesario.
- Revisar y actualizar accesos técnicos cuando se produzcan cambios o incidencias.
- Detectar, registrar y gestionar incidencias técnicas y de seguridad que afecten a los sistemas.
- Colaborar en la resolución de incidentes y en su análisis técnico.
- Escalar al Responsable del Sistema y al Responsable de Seguridad aquellas incidencias que puedan afectar a la seguridad o disponibilidad del servicio.
- Ejecutar y supervisar las copias de seguridad de los sistemas y datos, conforme a los procedimientos establecidos.
- Verificar periódicamente la correcta ejecución de los backups.
- Colaborar en las pruebas de restauración y recuperación ante incidentes o fallos.

- Ejecutar cambios técnicos autorizados en los sistemas.
- Garantizar que los cambios se realizan siguiendo los procedimientos de control de cambios.
- Mantener la trazabilidad de las modificaciones realizadas.
- Asegurar el correcto registro de las actividades administrativas relevantes.
- Conservar evidencias técnicas relacionadas con accesos, cambios, incidencias y operaciones.
- Facilitar la información necesaria para auditorías internas o externas.
- Comunicar al Responsable del Sistema y al Responsable de Seguridad cualquier debilidad, incidencia o anomalía detectada.
- Colaborar en análisis de riesgos técnicos y en la implantación de medidas correctoras.
- Apoyar técnicamente auditorías, revisiones y controles del ENS.

Responsable de Seguridad Física

Este perfil dispone de las siguientes funciones:

- Definir, implantar y supervisar las medidas de seguridad física necesarias para proteger las instalaciones, dependencias, zonas críticas y activos que soportan los sistemas de información.
- Garantizar el control de accesos físicos a las instalaciones y áreas sensibles, asegurando que dichos accesos están autorizados, registrados y revisados periódicamente.
- Velar por la protección de los sistemas frente a amenazas de origen físico, tales como accesos no autorizados, robos, sabotajes, daños accidentales o catástrofes.
- Coordinar la gestión de los incidentes de seguridad física, asegurando su registro, análisis y comunicación a los responsables correspondientes.
- Supervisar que las condiciones ambientales e infraestructurales (suministro eléctrico, climatización, protección contra incendios u otros riesgos físicos) son adecuadas para garantizar la continuidad de los sistemas de información.
- Colaborar en la identificación y evaluación de riesgos de seguridad física y en la definición de medidas correctoras o de mitigación.
- Participar en auditorías internas, revisiones y evaluaciones relacionadas con la seguridad física en el marco del Esquema Nacional de Seguridad.

Delegado de Protección de Datos

El Delegado de Protección de Datos (DPO) actúa como figura de supervisión y asesoramiento en materia de protección de datos personales, coordinándose con los responsables definidos en el Esquema Nacional de Seguridad.

Funciones:

- Asesorar a la organización y a los responsables ENS sobre las obligaciones en materia de protección de datos personales aplicables a los sistemas de información incluidos en el alcance del ENS.
- Supervisar que los tratamientos de datos personales incorporados en los sistemas de información cumplen los principios de protección de datos y las medidas de seguridad exigidas, de manera coherente con el nivel de seguridad ENS aplicable.
- Colaborar con el Responsable de Seguridad y el Responsable del Sistema en la definición y revisión de medidas de seguridad que afecten a tratamientos de datos personales.
- Participar, cuando proceda, en los análisis de riesgos y evaluaciones de impacto sobre la protección de datos (EIPD) relacionados con sistemas o servicios sujetos al ENS.
- Actuar como punto de contacto con las autoridades de control en materia de protección de datos y cooperar con estas en el ámbito de los sistemas de información cubiertos por el ENS.
- Asesorar en la gestión de incidentes de seguridad que afecten a datos personales, incluyendo la evaluación de su impacto y la necesidad de notificación conforme a la normativa de protección de datos.

7.2 Comité de Coordinación de Seguridad de la Información

Se ha constituido un Comité de Coordinación del SGSI (Sistema de Gestión de Seguridad de la Información).

Las funciones y responsabilidades del Comité de Coordinación del SGSI se detallan a continuación:

- Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.
- Gestionar y coordinar los aspectos relacionados con la Seguridad de la Información (documentar, apoyar en la implantación, efectuar mantenimiento y comunicar las decisiones tomadas).
- Reunir la información necesaria para la comprobación de todos los puntos recogidos en las normas de referencia, desde el análisis previo.
- Difundir a todos los miembros de la organización, los cambios acaecidos en la Política de Seguridad de la Información.

- Fomentar la implementación de las acciones en materia de seguridad y sus resultados.
- Participación en la definición y seguimiento de los objetivos de seguridad de compañía.
- Analizar y resolver incidencias y no conformidades detectadas, y proponer/validar el plan de trabajo/acciones correctivas asociadas.
- Identificar las necesidades de suministro/dotación de los recursos, internos y externos, necesarios para la correcta gestión del Sistema de Gestión Integrado.
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas.
- Mantener actualizada la documentación.
- Clasificación de la información y participación en la gestión de activos.
- Participar en la asignación de funciones y responsabilidades específicas de Seguridad de la Información.
- Colaborar en la elaboración y mantenimiento del Plan de Continuidad del Negocio.
- Definir los indicadores de seguridad, relativos a la eficiencia y eficacia, y realizar el seguimiento de los resultados para ayudar en la toma de decisiones oportunas.
- Establecer y aprobar el calendario de auditorías internas en materia de seguridad.
- Iniciar las acciones para prevenir las incidencias y No conformidades.
- Revisar y seguir las acciones correctivas, para asegurarse que éstas se llevan a cabo convenientemente.
- Establecer y proponer el plan anual de formación de la Seguridad de la Información, en función de las necesidades detectadas.
- Evaluación de riesgos de compañía.
- Participar en la revisión del sistema por la dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.

7.3 Procedimientos de designación

Es función de la Dirección de la Compañía designar:

- Al Responsable de la Información y de Servicio.

- Al Responsable de la Seguridad que debe reportar directamente a la Dirección y, al Comité de Coordinación del SGSI.
- Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de Seguridad.

Los nombramientos podrán ser revisados cada dos años, actualizándose cuando algunos de los puestos queden vacantes o por un incumplimiento reiterado de las funciones de alguno de sus miembros, previo apercibimiento y aplicación del régimen disciplinario.

Lexer debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

7.4 Resolución de conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité de Coordinación de Seguridad de la Información.

8. *Tratamiento de datos personales*

Lexer trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento, conforme a ello se evalúan los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

Lexer ha aprobado una Política de protección de datos personales que establece los principios y pautas de actuación que deben regir en la Compañía en materia de protección de datos personales, garantizando, en todo caso, el cumplimiento de la legislación vigente aplicable.

9. *Gestión de riesgos*

Todos los sistemas afectados por esta Política están sujetos a 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 se produzcan cambios en la información manejada,

- cuando se produzcan cambios en los servicios prestados,
- cuando ocurra un incidente grave de seguridad,
- cuando se reporten vulnerabilidades graves,
- y cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Coordinación de Seguridad de la Información 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.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

10. *Desarrollo de la política de seguridad de la información*

El cumplimiento de los objetivos marcados en esta Política de Seguridad se complementará con diversas normativas y recomendaciones de seguridad (manuales y procedimientos generales y específicos, instrucciones de trabajo, informes, registros y evidencias electrónicas). El Comité de Coordinación de Seguridad de la Información es responsable de su revisión y/o mantenimiento, proponiendo, si es necesario, mejoras al mismo.

La revisión anual de la presente Política corresponde a dicho Comité proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

La normativa de seguridad y, especialmente, la Política de Seguridad de la Información serán conocidas y estarán a disposición de todos los miembros de la empresa, en particular de quienes utilicen, operen o gestionen los sistemas de información y comunicación.

11. *Obligaciones del personal*

Todos los miembros de Lexer tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad del Comité de Coordinación de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC podrán recibir 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.

12. *Terceras partes*

Cuando Lexer preste servicios a otras entidades, se les hará partícipes de los principios recogidos en esta Política de Seguridad de la Información, a través del correspondiente acuerdo, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando Lexer utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad a través del correspondiente contrato de arrendamiento de servicios o NDA, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos críticos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la Lexer pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

13. *Gestión de incidentes de seguridad*

Lexer dispone de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14. *Categorización del sistema según ENS*

De acuerdo con lo establecido en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, el sistema de información de Lexer ha sido categorizado con un nivel de seguridad MEDIO para las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Esta categorización ha sido determinada atendiendo a la naturaleza de los servicios prestados, la información gestionada y el impacto potencial derivado de una pérdida de seguridad. La presente Política se aplica a todos los activos, servicios y procesos incluidos dentro del alcance del sistema categorizado.

15. *Objetivos de Seguridad ENS*

En cumplimiento del Esquema Nacional de Seguridad, Lexer establece los siguientes objetivos de seguridad:

- Prevenir la materialización de amenazas que afecten a la información y los servicios.
- Detectar de forma temprana actividades o comportamientos anómalos.
- Responder de manera eficaz ante incidentes de seguridad, minimizando su impacto.
- Conservar la información y garantizar la continuidad de los servicios esenciales.
- Recuperar los servicios con la menor interrupción posible.

Estos objetivos se aplican en todo el ciclo de vida de los sistemas de información.

16. *Compromiso de la Dirección*

La Dirección de Lexer manifiesta su compromiso con el cumplimiento del Esquema Nacional de Seguridad, garantizando:

- La dotación de recursos necesarios para implantar y mantener las medidas de seguridad.
- El apoyo institucional a las funciones del Responsable de la Seguridad y del Comité de Coordinación del SGSI.

- La integración de la seguridad en los procesos estratégicos, operativos y tecnológicos.
- La supervisión del estado de seguridad y de la mejora continua del sistema.

La Dirección asume la responsabilidad última del cumplimiento del ENS.

17. *Auditoría ENS*

Lexer realizará auditorías de seguridad ENS con una periodicidad mínima bienal, así como auditorías internas adicionales que garanticen la supervisión continua del sistema y el cumplimiento del marco legal aplicable.

18. *Aprobación de la política y entrada en vigor/efectividad*

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Coordinación de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Coordinación de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.