Política de Seguridad de la Información

Índice

1. INTRODUCCIÓN

ENAIRE, Ente Público Empresarial adscrito al Ministerio de Transportes, Movilidad y Agenda Urbana, tiene encomendada como misión, entre otras, la planificación, dirección, coordinación, explotación, conservación y administración del tráfico aéreo, de los servicios de telecomunicaciones e información aeronáutica, así como de las infraestructuras, instalaciones y redes de comunicaciones del sistema de navegación aérea, con el objetivo de que la prestación del servicio sea segura, eficaz, continuada y sostenible.

Tras la publicación del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información desarrollado a través del Real Decreto 43/2021, con fecha 30 de noviembre de 2018, ENAIRE es designado Operador Crítico y de Servicios Esenciales, destacando así la relevancia de los servicios prestados a sus clientes y la sociedad en su conjunto.

ENAIRE, fiel a sus principios de seguridad, calidad y eficiencia, declara su firme compromiso con la consecución y mantenimiento de los más altos niveles de ciberseguridad, tanto en sus sistemas operacionales directamente involucrados en la provisión de servicios de navegación aérea, como en los sistemas de información corporativos de soporte a la gestión empresarial y apoyo a la navegación aérea.

ENAIRE, a través de sus diferentes unidades, promoverá y garantizará la supervisión y monitorización continua de toda su infraestructura tecnológica, servicios prestados e información manejada, abarcando desde entornos de índole ofimática hasta los más críticos de naturaleza operacional.

Para ello, a nivel técnico se dispondrá de mecanismos eficaces de prevención, detección, respuesta y conservación de la información y servicios de la organización, ante incidencias de ciberseguridad a través de las unidades técnicas correspondientes, tanto a nivel centralizado como regional.

La Oficina de Ciberseguridad, adscrita a la División de Seguridad, coordinará los recursos corporativos, desarrollará y mantendrá el Sistema de Gestión de la Seguridad de la Información (SGSI), velará por el adecuado cumplimiento normativo y actuará en calidad de interlocutor y representante de ENAIRE ante organismos externos de referencia en la materia.

La Política de Seguridad de la Información se alinea con las Normas ISO/IEC 27000, 27001 y 27002 de Seguridad de Sistemas de Información, las normativas europeas y nacionales de Protección de Datos de carácter personal (LOPDGDD y RGPD), el RD 311/2022 que regula el Esquema Nacional de Seguridad (ENS) y el RD-Ley 12/2018 de Seguridad de las Redes y Sistemas de Información, junto con el RD 43/2021 que lo desarrolla, estructurando la gestión eficiente y eficaz de la seguridad de acuerdo a aquellas normas y a las buenas prácticas del sector, conforme con la mismas.

2. OBJETO Y ÁMBITO DE APLICACIÓN

La presente Política de Seguridad de la Información tiene por objeto ser el punto de partida del SGSI (Sistema de Gestión de la Seguridad de la Información) de ENAIRE y proporcionar el marco de actuación de la organización en Seguridad de la Información, teniendo en cuenta las actividades y servicios de la empresa, organización, ubicación, activos, tecnología, cadena de suministro, el entorno actual y previsto de amenazas para la Seguridad de la Información, la legislación, normativas vigentes y contratos, la estrategia de gestión de riesgos, así como la planificación de objetivos y metas.

El objetivo del SGSI y por tanto de la Política de Seguridad es la protección de la Información y los servicios, garantizando su autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad, así como la de los activos de procesamiento, transmisión y almacenamiento de información.

La presente Política de Seguridad de la Información será de difusión, conocimiento y aplicación a todo el personal propio o externo que tenga acceso a la información de ENAIRE y a todas las actividades, servicios y recursos tecnológicos que ENAIRE pone a disposición de la organización para el desarrollo del propio negocio. Por tanto, la presente Política afecta a toda la organización, incluidas las personas que integran el Consejo Rector y el Comité de Dirección, y en concreto, a los Sistemas de Información que soportan los servicios y los procesos que son necesarios para desarrollar y cumplir con los objetivos de negocio.

3. PRINCIPIOS DE ACTUACIÓN Y COMPROMISOS

3.1. Propósito, Misión y Visión

El **propósito** de ENAIRE en materia de ciberseguridad radica en reducir el riesgo y avanzar en la ciberresiliencia, tanto de sus propios servicios y operaciones, como en el ámbito del sector a nivel nacional y europeo.

La **visión** de ENAIRE en relación con la ciberseguridad es ser una organización de muy alta ciberresiliencia en los servicios de Navegación Aérea, con una gran capacidad de resistencia y recuperación frente a un panorama global de amenazas en constante evolución.

La **misión** de la ciberseguridad en ENAIRE es fortalecer la eficiencia, disponibilidad y seguridad de los servicios de Navegación Aérea en España y Europa mediante el despliegue de capacidades de ciberseguridad, la experiencia y el conocimiento, la colaboración y compartición de información con los distintos agentes del sector y la mejora continua en los procesos, tecnologías y concienciación.

Con el fin de alcanzar su Propósito, Misión y Visión, ENAIRE establece los siguientes principios generales para la Seguridad de la Información:

1. Seguridad como proceso integral: La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, estratégicos, jurídicos y organizativos, relacionados con el sistema y sus interconexiones, encaminada a garantizar la prevención, detección, respuesta y conservación ante las amenazas e incidentes. El SGSI de ENAIRE formará parte del Sistema Integrado de Gestión (SIG) y estará integrado con los procesos de la organización (Gobierno, Servicios y Apoyo) y con la estructura de gestión global y, por lo tanto, la Seguridad de la Información será tenida en cuenta durante el diseño de los procesos y los sistemas a lo largo de todo su ciclo de vida.
2. Gestión de la seguridad basada en los riesgos: El SGSI de ENAIRE preservará la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información y los servicios mediante la aplicación de un proceso continuo y permanentemente actualizado de análisis y gestión de riesgos, considerando asimismo a los proveedores y terceros involucrados.
3. Prevención, detección, respuesta y conservación: La gestión de incidentes de seguridad contempla medidas de seguridad que implementan mecanismos de prevención, detección, registro, clasificación, análisis, respuesta, comunicación y conservación de cualquier incidente o desviación significativa de los parámetros establecidos como normales. De manera complementaria, la continuidad de negocio formará parte del Sistema de Gestión, conforme a las necesidades de la organización, los controles establecidos y los correspondientes planes de recuperación y aseguramiento de los servicios más críticos.
4. Existencia de línea de defensa: La estrategia de protección de los Servicios en ENAIRE se basa en múltiples capas de seguridad, constituidas por medidas de naturaleza organizativa, tecnológica,

física y lógica, de tal manera que si alguna se viese comprometida, el posible impacto final sea mínimo.

5. Vigilancia continua y reevaluación periódica: La organización se compromete a mantener y mejorar de manera continua su SGSI mediante procesos de vigilancia continua y evaluaciones permanentes de la seguridad, con la finalidad de conocer el estado de seguridad de los sistemas y el tratamiento de desviaciones y excepciones (monitorizaciones, auditorías, indicadores, no conformidades, planes de tratamiento de riesgos…).
6. Diferenciación de responsabilidades: ENAIRE organiza su seguridad en unidades organizativas y comités específicos, comprometiendo a todos los miembros de la dirección de la empresa. Designa diferentes roles de seguridad con responsabilidades diferenciadas, mecanismos de coordinación y resolución de conflictos.
7. Recursos: La organización determinará y asignará los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, incluyendo la adquisición y servicios de seguridad.
8. Evaluación del cumplimiento de objetivos: Se establecerán planes estratégicos y objetivos de seguridad de la información y se evaluará el cumplimiento de los resultados previstos por el SGSI.
9. Formación y concienciación: Se pondrán en marcha las acciones de formación y concienciación en Seguridad de la Información que se consideren necesarias para asegurar la competencia en esta materia de los empleados de la organización, atendiendo a las necesidades específicas de cada perfil según sus funciones.
10. Difusión: La difusión de las buenas prácticas en materia de Seguridad de la Información, así como de esta Política y el refuerzo constante de los mensajes esenciales, es tarea crítica para lograr una correcta asimilación de principios fundamentales que alimenten el motor de conocimiento de ENAIRE.

3.2. Compromisos

3.2.1. Marco Legal y Regulatorio

La definición del Sistema de Navegación Aérea (SNA) y de los servicios y sistemas que lo componen se establece en el Real Decreto 931/2010.

ENAIRE está sometida a normativas específicas de Navegación Aérea, algunas de las cuales contemplan aspectos de seguridad de la información. En particular:

- Reglamento de Ejecución (UE) 2017/373, por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión.
- Reglamento (UE) 1029/2014, por el que se establecen requisitos relativos a la calidad de los datos aeronáuticos y la información aeronáutica para el Cielo Único Europeo.
- Reglamento (CE) 633/2007, por el que se establecen requisitos para la aplicación de un protocolo de transferencia de mensajes de vuelo utilizado a efectos de notificación, coordinación y transferencia de vuelos entre dependencias de Control del Tránsito Aéreo.
- Real Decreto (RD) 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3.2.2. Objetivos de Seguridad de la Información

Se establecerán los objetivos de Seguridad de la Información, en las funciones y niveles pertinentes, que serán:

- Coherentes con la presente Política de Seguridad de la Información.
- Medibles.
- Consistentes con los resultados de las evaluaciones de riesgos.
- Documentados, comunicados y actualizados, según el procedimiento que se establezca al efecto.

Con carácter general, esta Política establece los siguientes objetivos:

- Cumplir con la legislación vigente en materia de seguridad de los Sistemas de Información.
- Asegurar la confidencialidad e integridad de los datos.
- Asegurar la disponibilidad de los Sistemas de Información.
- Asegurar la capacidad de respuesta ante situaciones de emergencia, restableciendo los servicios críticos en el menor tiempo posible.
- Garantizar la autenticidad de la información en aquellos procesos claves.
- Mantener una trazabilidad adecuada de la información de los Sistemas de Información, cuando sea preciso.
- Promover la formación y concienciación continuada de la Seguridad de la Información.
- Potenciar la implementación de buenas prácticas alineadas con el RD 311/2022 (Anexo II), el RD-Ley 12/2018 y la ISO/IEC 27002.

3.2.3. Organización de la Seguridad

La Dirección de ENAIRE aporta los recursos necesarios para garantizar la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los Sistemas de Información para el desarrollo normal de las actividades de los empleados y los servicios prestados a nuestros clientes. La Dirección constituye el Comité de Ciberseguridad y Seguridad Física que velará por el cumplimiento del SGSI y de los objetivos de Seguridad de la Información. En el documento “Organización de la Seguridad de la Información” se describe de forma detallada la estructuración, composición, funcionamiento y tareas específicas de la función de la Seguridad de la Información en la organización de ENAIRE.

3.2.4. Comité de Seguridad de la Información

El Comité de Ciberseguridad y Seguridad Física, denominado SECCIBE, será quien lidere la organización y promueva la cultura de Seguridad de la Información, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso o servicio prestado. El SECCIBE podrá formar parte de otros Comités de Gestión, pero será el responsable de coordinar, evaluar y proponer mejoras para la Seguridad de la Información y los servicios involucrados.

De igual modo, podrán existir subcomités de Seguridad de la Información, presididos por los Delegados de Seguridad de la Información, que deben seguir las directrices marcadas a nivel global. Estos órganos de gestión materializan el principio de cooperación que debe imperar en la organización de Seguridad de la Información de ENAIRE.

El SECCIBE se reunirá, al menos, con una periodicidad trimestral y sus funciones principales, entre otras, son las siguientes:

- Desarrollar y coordinar la estrategia de Seguridad de la Información y realizar el seguimiento de la ejecución.
- Asesorar a la organización en materia de Seguridad de la Información, resolviendo los conflictos de responsabilidad en dicha materia.
- Aprobar otras políticas, normas y procedimientos en materia de Seguridad de la Información.
- Promover la mejora continua del SGSI en coordinación con el responsable del Sistema Integrado de Gestión. Participar en la revisión del Sistema de Gestión.
- Recibir informes del estado de la seguridad física, lógica y operativa y su impacto en ENAIRE.
- Recibir informes del estado de implantación de la normativa referente a Infraestructuras Críticas en ENAIRE y adoptar medidas correctoras.
- Realizar el control y seguimiento de las acciones y tomas de decisión determinadas en anteriores Comités, así como analizar las posibles desviaciones.
- Reportar al Comité de Dirección.

3.2.5. Roles y Responsabilidades

La seguridad de la información se conforma principalmente en tres figuras organizativas diferenciadas. La designación y renovación de los miembros que ostenten los distintos roles y responsabilidades será potestad del Comité responsable de la Seguridad de la Información y ratificado por el Comité de Dirección. Estos nombramientos se revisarán cada dos años o cuando el puesto quede vacante.

- Responsable de Seguridad, enmarcado en la División de Seguridad, a través del jefe de División de Seguridad. Las principales atribuciones y responsabilidades son:
    - Mantener la Seguridad de la Información manejada y de los servicios prestados por los Sistemas de Información.
    - Promover campañas de formación y concienciación en materia de Seguridad de la Información.
    - Administrar el SGSI y la coordinación con el resto de las divisiones, autoridades y entidades externas en materia de Seguridad de la Información.
    - Realizar de forma continuada el Análisis de Riesgos, evaluando los impactos por los incidentes de seguridad y las actualizaciones y/o cambios en los sistemas y redes.
    - Gestionar y comunicar a las autoridades y organismos competentes los distintos incidentes de Seguridad de la Información acontecidos en la organización, basándose en la criticidad de los mismos.
    - Elaborar y mantener actualizada la documentación en materia de seguridad dentro de su ámbito de actuación.

- Responsable de Sistemas, enmarcado en la Dirección de Sistemas a través del Director de Sistemas. Las principales atribuciones y responsabilidades son:
    - Desarrollar, operar y mantener los Sistemas de Información durante todo el ciclo de vida, sus especificaciones, instalación y verificación de su correcto funcionamiento.
    - Definir las topologías y sistemas de gestión de los Sistemas de Información, estableciendo los criterios de uso y los servicios disponibles de los mismos.
    - Realizar la ejecución de las acciones necesarias para la aplicación de las medidas de Seguridad de la Información dimanantes del proceso de mejora continua y del Plan de Tratamiento de Riesgos del SGSI que correspondan a sus áreas.
- Responsables de Información y Servicio, enmarcados en las Direcciones responsables de un Servicio en particular. Las principales atribuciones y responsabilidades son:
    - Establecer los requisitos en materia de Seguridad de la Información y del Servicio que gestionan en su ámbito funcional de responsabilidad.
    - Definir los distintos niveles de seguridad, participando activamente en el Análisis de Riesgos y realizando la valoración de los activos de su responsabilidad en las dimensiones de seguridad contempladas.
    - Colaborar en la elaboración de la normativa de Seguridad de la Información dentro de su ámbito de actuación.

Asimismo, ENAIRE, como Operador de Infraestructuras Críticas y de Servicios Esenciales, dispone de un Responsable de Seguridad y Enlace, un Responsable de la Seguridad de la Información y, para cada una de dichas infraestructuras, un Delegado de Seguridad.

El Responsable de Seguridad y Enlace representará a ENAIRE ante los organismos del Estado en todas las materias relativas a la seguridad de sus infraestructuras y de los diferentes planes derivados, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto.

Por su parte, el Responsable de la Seguridad de la Información actuará como punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información, y como punto de contacto especializado con el CSIRT de referencia.

Finalmente, cada Delegado de Seguridad constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica de su competencia, encauzando las necesidades operativas e informativas que se refieran a aquella.

Sin perjuicio de lo anterior, todo personal interno o externo de ENAIRE es responsable de la seguridad y uso de la información dentro de su ámbito funcional y orgánico de desempeño, de forma tal que existe una corresponsabilidad compartida entre empleados y directivos y la organización de seguridad. El incumplimiento de esta Política y/o de la normativa interna aplicable, tanto en materia de seguridad y uso de la información como de recursos tecnológicos, podrá derivar en la aplicación de las medidas disciplinarias que se estimen oportunas, conforme al procedimiento establecido, en función de la magnitud, impacto y características de la infracción.

3.2.6. Conformidad Legal

ENAIRE tiene el firme compromiso de velar por el cumplimiento de la legislación y normativa vigente en materia de protección y Seguridad de la Información considerando su objeto, razón social y finalidad de negocio. En ese sentido, la Dirección ha establecido como requerimiento de seguridad el pleno

cumplimiento de las obligaciones legales y contractuales, ligadas a la información y a los servicios. Los requisitos serán identificados y organizados para su correcta gestión en el documento “Legislación y Requisitos aplicables”.

Por la naturaleza y objeto de negocio de ENAIRE se deben cumplir leyes, normas y disposiciones legales sobre, al menos, aspectos de servicios de Navegación Aérea, seguridad de Infraestructuras Críticas y Servicios Esenciales, propiedad intelectual, protección de datos de carácter personal, retención y almacenamiento de información que tendrán prevalencia, cuando apliquen, sobre las directrices contenidas en esta Política de Seguridad de la Información.

Se considerarán también las normas que provengan de organismos supranacionales de los que España sea miembro y la normativa comunitaria y/o extracomunitaria, en razón a las áreas de prestación de servicios por parte de ENAIRE.

3.2.7. Estructura de la Documentación de Seguridad

El presente documento desarrolla la Política de Seguridad de la Información de alto nivel. A un nivel inferior, esta Política de Seguridad de la Información se apoyará en diversas políticas, normas y procedimientos de obligado cumplimiento sobre temas específicos que estarán estructurados para atender las necesidades de determinados grupos dentro de la organización (uso de los recursos tecnológicos, comunicación de incidentes, obligaciones y deberes…). El desarrollo, clasificación y tratamiento de la documentación de seguridad seguirá las pautas del proceso de Gestión Documental de ENAIRE.

Además, se definirán los objetivos que ENAIRE pretende conseguir con la aplicación de su Sistema de Gestión de Seguridad de la Información y que serán evaluados para determinar la efectividad del SGSI.

Como parte del SGSI, se desarrollarán diferentes procedimientos específicos que alcanzarán el detalle técnico necesario para la aplicación de los controles de seguridad.

Todos estos documentos estarán accesibles para todos los empleados de la organización, tanto propios como externos, en la medida que sea necesario basándose en su “necesidad de conocer” para el correcto desempeño de sus funciones en la empresa. En ese sentido, todos los miembros de ENAIRE tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad.

3.2.8. Gestión de Riesgos

ENAIRE aplicará un proceso de gestión de riesgos de Seguridad de la Información que:

- Establezca y mantenga criterios sobre riesgos de Seguridad de la Información, incluyendo:
    - Los criterios de aceptación de riesgos.
    - Los criterios para llevar a cabo las evaluaciones de riesgos.
- Asegure que las sucesivas evaluaciones de riesgos generen resultados consistentes, válidos y comparables.
- Identifique las amenazas de Seguridad de la Información.
- Analice las amenazas de Seguridad de la Información:
    - Valorando las posibles consecuencias que resultarían si las amenazas identificadas llegasen a materializarse.
    - Valorando de forma realista la probabilidad de ocurrencia de las amenazas identificadas.
    - Determinando los niveles de riesgo.

- Evalúe los riesgos de Seguridad de la Información:
    - Comparando los resultados del Análisis de Riesgos con los criterios de riesgo establecidos.
    - Priorizando el tratamiento de los riesgos analizados.
- Efectúe un tratamiento de riesgos de Seguridad de la Información para:
    - Seleccionar las opciones adecuadas de tratamiento de riesgos teniendo en cuenta los resultados de la evaluación de riesgos.
    - Determinar las salvaguardas necesarias para implementar el tratamiento de riesgos elegido.
    - Elaborar un Plan de Tratamiento de Riesgos de Seguridad de la Información.

Los procesos de gestión de riesgos se efectuarán periódicamente a intervalos planificados, así como cuando se propongan o se produzcan modificaciones importantes. Se conservará registro documental de todos los procesos de gestión de riesgos.

3.2.9. Auditoría y Continuidad de Negocio

Los Sistemas de Información, de manera total o parcial, se someterán periódicamente a auditorías internas y externas con la finalidad de verificar su correcto funcionamiento, determinando grados de cumplimiento y recomendando medidas correctoras para una mejora continua.

La administración de la continuidad de los servicios es un proceso crítico que debe considerar involucrar a toda la organización. El desarrollo e implantación de los Planes de Continuidad garantizarán que los servicios indispensables puedan restablecerse en los plazos requeridos, incluyéndose controles destinados a identificar y reducir riesgos, así como atenuar las consecuencias eventuales de las posibles interrupciones del servicio. Periódicamente dichos Planes deberán ser probados, revisados y actualizados para asegurar la continuidad de su eficacia.

3.2.10. Datos de Carácter Personal

ENAIRE realiza el tratamiento de los datos de carácter personal, para lo cual dispone de un Manual de Tratamiento de Datos Personales conforme al Reglamento (UE) 2016/679. Este Protocolo, incluido el análisis de riesgo del tratamiento de datos personales, recoge todos los elementos iniciales requeridos para dar cumplimiento a la normativa de protección de datos, definiendo y estableciendo aspectos esenciales, para mantener la diligencia debida del responsable.

A todos los efectos, esta política da cumplimiento Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Así mismo, también da cumplimiento a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales (LOPDGDD).

Todos los sistemas de información de ENAIRE se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Protocolo de Seguridad. De igual modo, adoptará las medidas técnicas y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso, destacando la Unidad Central de Protección de Datos (UCPD) como centro de apoyo y asesoramiento específico en la materia.

3.2.11. Confidencialidad de la Información

Tanto los empleados propios como terceras partes (ej. Asistencias Técnicas o Servicios Externos) que trabajen para o en nombre de ENAIRE deben preservar y proteger la información, datos, servicios y activos de ENAIRE, utilizándolos estrictamente para el cumplimiento de sus funciones y comprometiéndose a no divulgar información, datos, imágenes o contenidos de cualquier naturaleza o formato (digital o material) propiedad de ENAIRE o relacionados con ENAIRE, sus empleados, recursos, sistemas, operaciones, instalaciones o infraestructuras, que hayan tenido acceso o conocimiento gracias a su relación con ENAIRE, sin autorización expresa y formal, conforme a la normativa interna de Uso de Recursos Tecnológicos.

ENAIRE velará por el cumplimiento de estos principios, aplicando las restricciones oportunas y, en su caso, el régimen disciplinario.

4. MECANISMOS DE SUPERVISIÓN

La Dirección ha establecido las líneas estratégicas que garantizan la materialización de estos compromisos en actuaciones y resultados, y se compromete a proporcionar los recursos necesarios para prestar nuestros servicios, gestionando los recursos económicos con criterios de eficiencia.

Dada la relevancia de las cuestiones relativas a la Seguridad de la Información, se atribuyen funciones específicas a Comités especializados como el Comité de Ciberseguridad y de Seguridad Física de ENAIRE.

El Comité de Dirección supervisará la promoción y despliegue de esta Política, e informará a través del Director General de su avance al Consejo Rector, cuando sea pertinente, conforme a los procesos establecidos para su Revisión en el marco del Sistema Integrado de Gestión.

5. PUBLICIDAD Y DIVULGACIÓN

Esta Política está respaldada por la Alta Dirección y se mantiene como información documentada.

ENAIRE cuando preste servicios a otros organismos o utilice servicios de terceros, se les hará partícipe de esta Política de Seguridad de la Información y de la normativa de seguridad relacionada a dichos servicios, estableciéndose canales de coordinación y reporte.

En cumplimiento con los requisitos de las Normas internacionales y prácticas de transparencia, esta Política estará a disposición de todas las partes interesadas en la web de ENAIRE, para su información y consulta.

Igualmente, se realizará la comunicación oportuna de difusión y comunicación interna mediante las herramientas existentes, para su comprensión y aplicación dentro de la organización, con el fin de confirmar el compromiso de ENAIRE con nuestro personal, el desarrollo y progreso que garanticen el futuro del sector aeronáutico y de la sociedad española, fomentando su divulgación para que sea entendida por todas las personas que actúan en nombre de ENAIRE.

6. APROBACIÓN Y VIGENCIA

Tras su presentación en el Comité de Dirección de 19 de abril de 2023, la presente Política ha sido aprobada por el Consejo Rector de ENAIRE en su reunión de 26 de abril de 2023, entrando en vigor desde esta última fecha, y permanecerá vigente en tanto no se produzca ninguna modificación en la misma la cual será comunicada adecuadamente.

Esta Política será objeto de revisión y actualización cuando sea necesario para adecuarla a los eventuales cambios normativos, sociales, económicos u organizativos.