Con su Sistema de Gestión de Seguridad de la Información

Liderazgo de ENAIRE en Ciberseguridad

■ *Texto: Gerardo Sarmiento. Responsable de la Oficina de Ciberseguridad de ENAIRE*
Imágenes: ENAIRE

El gestor nacional de navegación aérea está reconocido desde 2018 como entidad proveedora de servicios esenciales de la mayor criticidad para el Estado y la sociedad. Sus sistemas de tratamiento y gestión de planes de vuelo, tráfico aéreo, comunicaciones, navegación, vigilancia, meteorología, información aeronáutica, supervisión y explotación técnica están certificados en Categoría Alta en el Esquema Nacional de Seguridad, la más completa y exigente certificación en la materia.

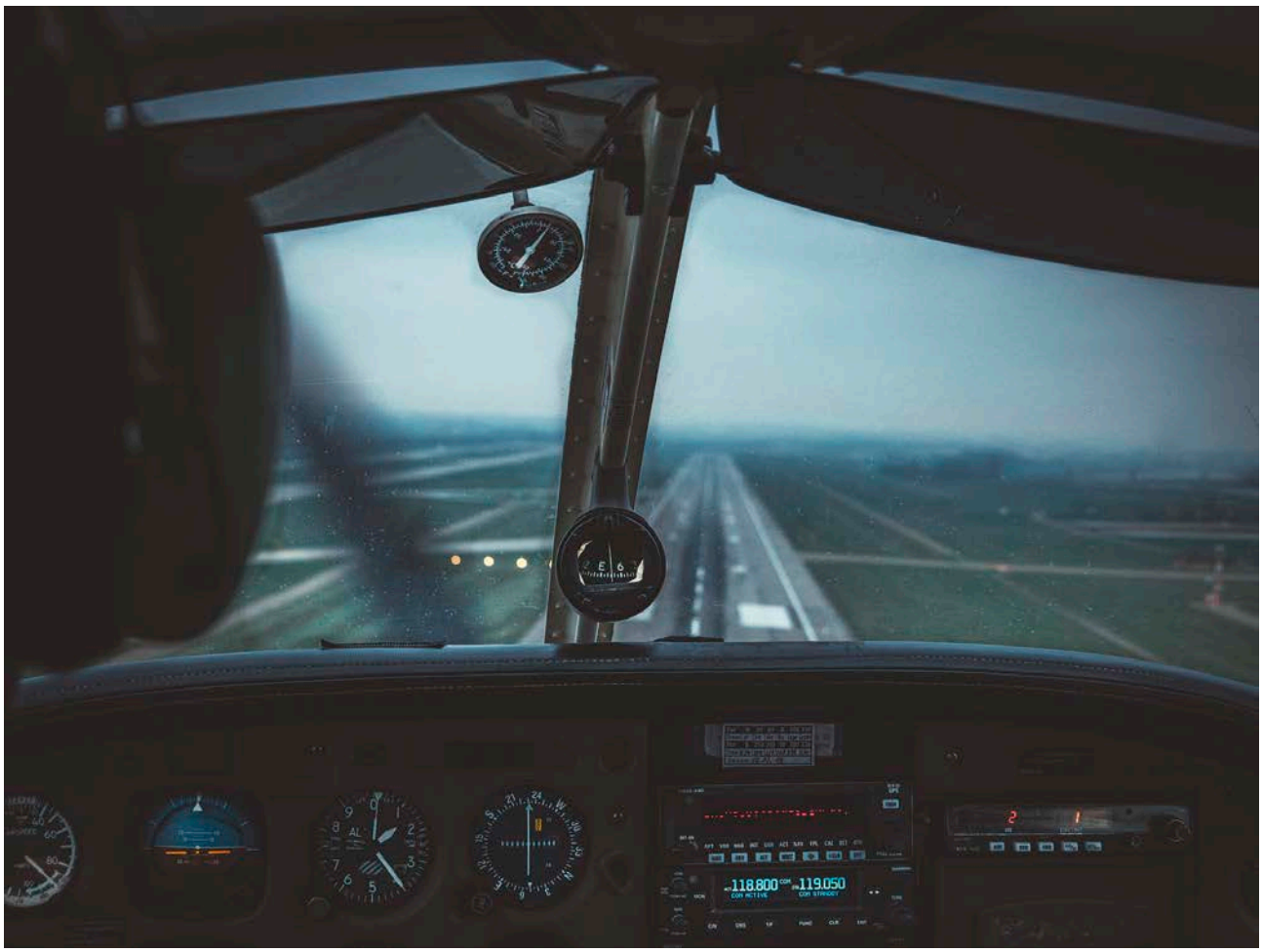
El desarrollo de las Tecnologías de la Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo.

Según se indica en la Estrategia de Ciberseguridad Nacional, el ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de Tecnología de la Información –incluida Internet–, las redes y los sistemas de información y de telecomunic ciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas.

El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales que, desde diferentes ámbitos, confluyen en un mismo concepto: la ciberseguridad.

El mundo de la aviación no es ajeno a esta evolución. Muy al contrario, los sectores del transporte aéreo en general y de la navegación aérea en particular están altamente tecnificados, siendo motores y partícipes de esta transformación de un modo muy activo. El alto grado de demanda del sector, unido a la criticidad de sus operaciones, requiere el más alto nivel de concienciación y compromiso por parte de todos.

Algunos de los riesgos y amenazas que se desarrollan en el ámbito aeronáutico son los tradicionales, derivados de la interferencia deliberadamente ilícita de cualquier agente externo con fines criminales. Contra ellos se dispone de una potente estructura de seguridad que proporciona a la sociedad un nivel de protección elevado, si bien siempre es potencialmente mejorable.



Las operaciones aeronáuticas exigen un nivel de protección y seguridad elevado.

No obstante, existen nuevas amenazas derivadas de la evolución tecnológica del entorno en su conjunto que requieren el desarrollo de nuevos procedimientos y sistemas orientados a la adecuada gestión y mitigación de sus riesgos asociados.

Dicha tecnología está conformada por sistemas de información y telecomunicaciones integrados en redes, en los que se basan tanto sus medios y servicios aéreos (plataformas, radares embarcados, comunicaciones aire-aire, etc.), como terrestres (servicios aeroportuarios, radares y sistemas de control aéreo, sistemas de comunicaciones tierra-tierra y tierra-aire, etc.) o satelitales (navegación basada en geolocalización, etc.).

Bien por omisión, fallo u obsolescencia, esta tecnología es susceptible de presentar carencias en términos de diseño, implementación o mantenimiento que pueden originar graves vulnerabilidades en los mismos.

Protección ante ciberataques

No debe olvidarse que los ciberataques son una actividad de máxima rentabilidad, dada la facilidad y bajo coste con que se puede atacar la integridad de los datos de estos sistemas. Un ataque efectivo podría desembocar bien en su inoperatividad total o parcial, bien en la falta de fiabilidad por la falsedad de la información que contengan, lo que podría desencadenar desde un mal funcionamiento al colapso de determinados sistemas y servicios, llegando incluso a provocar accidentes mortales.

Esta realidad hace imprescindible la protección de los medios y servicios del sector contra ciberataques, atendiendo a las principales características de la información y los sistemas de navegación aérea, como son la integridad, la disponibilidad y la autenticidad.

La ausencia de modificaciones no autorizadas de la información es de vital importancia, no sólo

desde el punto de vista de alteración o eliminación de datos, sino también de la creación o reactuación de mensajes transmitidos que puedan comprometer las actividades en todos los ámbitos.

Asimismo, los recursos necesarios deben estar disponibles en todo momento, garantizando tanto la continuidad del servicio como la seguridad de todas las operaciones.

Por último, la validez de la información, intrínsecamente vinculada a la identidad del interlocutor que la genera, es fundamental en términos de confiabilidad de los datos gestionados, debiendo establecerse las medidas oportunas que la certifiquen.

Confidencialidad, trazabilidad y privacidad

Adicionalmente, aun no siendo parámetros de la máxima criticidad en el sector (dada la naturaleza pública de gran parte de la información gestionada), otras cualidades deben ser tenidas en consideración: la confidencialidad, la trazabilidad y la privacidad.

Se debe velar por la limitación de acceso a la información que por su naturaleza así lo requiera, restringiéndolo exclusivamente a las entidades y personas autorizadas e impidiendo cualquier forma de divulgación no controlada.

De forma complementaria, cuando sea necesario, se deben establecer los procedimientos necesarios que permitan conocer el histórico, ubicación, trayectoria y/o evolución de la información a lo largo de su ciclo de vida.

Finalmente, la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos es, a día de hoy, un pilar esencial en la gestión de la seguridad de la información.

ENAIRE está designado como operador crítico desde 2015, en 2018 obtuvo la certificación del Esquema Nacional de Seguridad, y en 2020 ha conseguido la Categoría Alta.

Marco normativo

A la vista de lo anterior queda patente que la navegación aérea es, sin lugar a dudas, uno de los sectores en los que la seguridad adquiere un mayor protagonismo. No en vano, a pesar de la gran complejidad de sus operaciones y los sistemas que las sustentan, las cifras lo avalan como el medio de transporte más seguro del mundo.

Ello se traduce en que el marco normativo en el cual se desarrollan las actividades de ENAIRE está fuertemente regulado, debiendo cumplir leyes, normas y disposiciones legales sobre, al menos, aspectos de servicios de navegación aérea, propiedad intelectual, protección de datos de carácter personal, retención y almacenamiento de información, entre otros.

Esta circunstancia queda plenamente ratificada por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) que, en virtud de diferentes leyes y reales decretos, designa a ENAIRE como Operador Crítico en 2015 y, posteriormente, Operador de Servicio Esencial en 2018. En definitiva, tanto en el ámbito operacional como en el físico, la seguridad forma parte del ADN de ENAIRE. Teniendo en cuenta el imparable auge de las nuevas tecnologías, así como el marcado carácter innovador de la propia aviación, a todo ello se une también la ciberseguridad.

En 2015, tras la designación como Operador Crítico, nace la Oficina de Ciberseguridad de ENAIRE. Esta unidad asume el reto de homogeneizar y consolidar de manera centralizada lo que ya se venía realizando en años anteriores y aporta una capa adicional de coordinación corporativa de iniciativas, optimización de recursos y alineación procedimental y normativa. Fruto de ello, en 2018, ENAIRE obtiene un primer Certificado de Conformidad con el Esquema Nacional de Seguridad (ENS), hecho que supone un importante hito en este ámbito y sienta las bases de un Sistema de Gestión de Seguridad de la Información, integral y global, a partir del cual desplegar un ambicioso abanico de proyectos e iniciativas en materia de ciberseguridad.

A partir de ahí, diferentes directivas, decretos, leyes, reglamentos o estrategias se van sumando a un escenario normativo cada vez más completo y complejo. En primer lugar, la Directiva (UE) 2016/1148 (*Network and Information Security - NIS*) sienta, en términos europeos, las bases de una visión compartida de la Seguridad de las Redes y Sistemas de Información que, en su transposición al ordenamiento jurídico nacional, da lugar al Real Decreto-ley 12/2018 con idéntica denominación. Como consecuencia de ello se produce la designación de ENAIRE como Operador de Servicios Esenciales, recalcando aún más si cabe su papel protagonista en el entramado socioeconómico nacional y, por extensión, la relevancia de la seguridad y continuidad de sus servicios.

Por otra parte, una referencia fundamental en el contexto de la provisión de servicios de navegación aérea es el 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. También esta norma contempla requisitos de ciberseguridad, cuyo cumplimiento -como en los restantes casos anteriores- queda plenamente satisfecho con la Certificación de Conformidad con el Esquema Nacional de Seguridad.

ENAIRE en el mundo

Algunas de las anteriores referencias normativas, enmarcadas en el plano legislativo internacional, ponen de manifiesto la clara globalización del negocio de la navegación aérea. ENAIRE, en su destacada vocación de proveedor mundial líder en el sector, también comparte este espíritu y presta sus servicios fuera de nuestras fronteras, a través de empresas participadas, como GroupEAD o EGNOS.

Asimismo, colabora activamente en diferentes equipos e iniciativas punteras del sector aeronáutico. Un buen ejemplo de ello es el consorcio internacional SACTA-iTEC, vinculado con los desarrollos tecnológicos más avanzados en el campo del control de tráfico aéreo, en cuya implementación se integran exigentes requisitos de ciberseguridad desde la más temprana fase de diseño.

De hecho, la consolidación de la ciberseguridad como un elemento de indiscutible calado es ya una realidad en el sector en todos los ámbitos. Organismos como la Organización de Servicios de Navegación Aérea Civil (CANSO) o la Organización Europea para la Seguridad del Control Aéreo (EUROCONTROL) son sólo algunos de los numerosos foros en los que ENAIRE participa activamente, cooperando en el desarrollo de mejores prácticas (*Standards of Excellence*), compartiendo información y aportando recursos para beneficio de toda la comunidad y los *stakeholders* que la conforman.

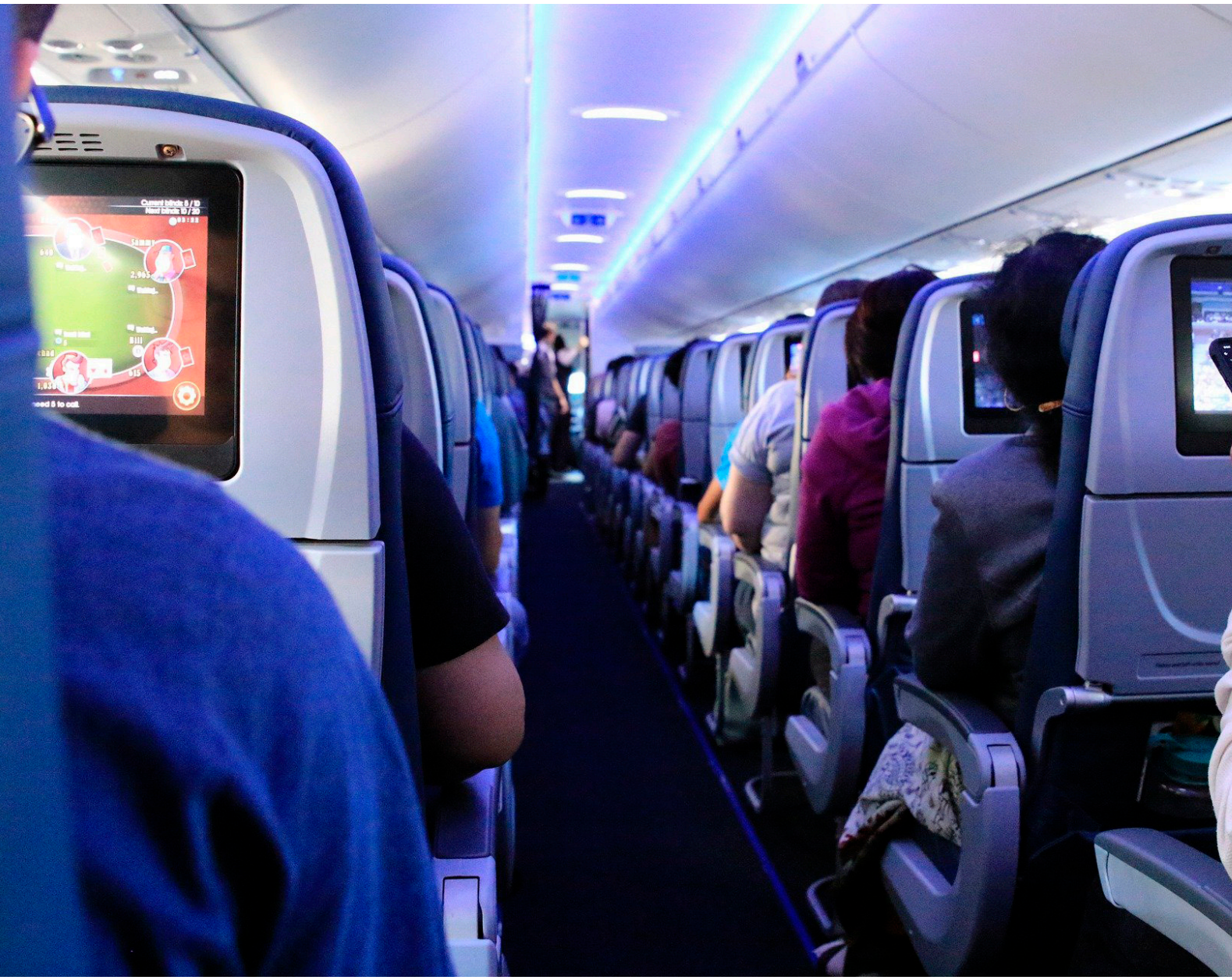
Programa Técnico de Seguridad

En junio de 2019, a través de su Programa Técnico de Seguridad, ENAIRE da un salto cualitativo en materia de protección de la información y los sistemas que soportan la sofisticada *maquinaria de relojería* que hace posible la navegación aérea. Este Programa se inscribe dentro del marco estratégico del Plan de Vuelo 2020 de ENAIRE y está alineado con la Estrategia Nacional de Ciberseguridad y la Estrategia de Seguridad Aeroespacial Nacional, figurando asimismo de manera destacada en el "Informe sobre la seguridad de los transportes y las infraestructuras", publicado por el Ministerio de Fomento en febrero de 2019.

A través de este nuevo Programa, ENAIRE refuerza aún más la arquitectura, ya de por sí robusta, de sus equipamientos TIC (Tecnologías de la Información y Comunicación), puntos neurálgicos del transporte aéreo. Se trata de una iniciativa esencial destinada a garantizar la adecuada continuidad del servicio y asegurar un nivel adecuado de protección de su información, así como de los sistemas y las comunicaciones que le dan soporte.

El Programa Técnico de Seguridad de ENAIRE comprende diferentes aspectos, abarcando personas, procesos, herramientas y tecnología, todo ello orientado a la gestión, tanto proactiva como reactiva, de las amenazas, vulnerabilidades y, en general, cualquier incidente de seguridad. Su objetivo último es minimizar el impacto de los mismos en sus redes y servicios, teniendo en cuenta la rápida evolución, tanto en complejidad como en número, de las amenazas sobre dichas tecnologías.

En primer lugar, el Programa establece mecanismos de detección y monitorización continua, mediante los cuales identificar vulnerabilidades, amenazas potenciales y su posible impacto en la organización, permitiendo una gestión proactiva de



Los proveedores de servicios de navegación aérea están obligados a unos estrictos requisitos en materia de ciberseguridad.

la seguridad. Para lograrlo, la adquisición e implantación de herramientas técnicas de última generación resulta imprescindible. La correlación centralizada de todos los eventos, la revisión periódica de la infraestructura, la detección temprana de cualquier intento de ataque y, finalmente, la consiguiente generación de alarmas -en aquellos casos en los que se constate la ocurrencia de cualquier anomalía- resultan cruciales.

Pruebas de seguridad

La ejecución de pruebas de seguridad sobre los activos de ENAIRE es otro elemento crítico dentro del alcance del proyecto, tanto desde la óptica de la auditoría (análisis pasivos) como del *hacking* ético (ensayos ofensivos de intrusión). Por último, la estrecha colaboración con organismos externos del máximo nivel, la vigilancia digital permanente y la integración de diferentes fuentes de información, de reconocido prestigio y fiabilidad, complementan el apartado preventivo.

En el supuesto de que se produzca cualquier incidente de seguridad, ENAIRE precisa dis-

poner de un equipo de respuesta capaz de minimizar el impacto en sus procesos y servicios prestados. Dicho equipo debe realizar las correspondientes investigaciones sobre las redes y puntos finales comprometidos que conduzcan a su pronta resolución, así como a la aplicación de aquellas medidas preventivas y correctivas que repercutan en una mejora en la ciberseguridad. La gestión de incidentes de seguridad es, por tanto, uno de los pilares básicos del Programa Técnico de Seguridad de ENAIRE, asumiendo que, en la práctica, su ocurrencia es inevitable. El concepto de resiliencia resulta ya imprescindible en el actual paradigma de la seguridad de la información, siendo la gestión de crisis un elemento fundamental en el proceso de recuperación ante cualquier interrupción o degradación del servicio.

Como ya se ha indicado con anterioridad, la Oficina de Ciberseguridad de ENAIRE es la responsable de liderar, gestionar, planificar y supervisar la ciberseguridad a escala corporativa. No obstante, ésta es una tarea compleja que requiere de la activa participación de las diferentes unidades técnicas. En este sentido, el Programa descrito también aporta un valor añadido, recogiendo la colaboración y contribución en ámbitos como el cumplimiento normativo o el desarrollo estratégico, entre otros.

En el plano de la monitorización, resulta evidente que la seguridad no se rige por horarios ni calendarios, tratándose de un servicio continuado 24 horas al día, 365 días del año. Para garantizar este elevado nivel de disponibilidad, el Programa Técnico de Seguridad de ENAIRE cuenta con un Centro de Operaciones de Seguridad (también conocido por sus siglas en inglés “SOC”), destinado a monitorizar sus sistemas de manera ininterrumpida. Ante cualquier circunstancia que potencialmente pueda comprometer la normal continuidad de las operaciones de nuestra organización, el SOC H24 constituye un servicio de seguridad permanente que garantiza la capacidad de monitorización y respuesta inmediatas, en la línea de lo demandado por una entidad como ENAIRE, proveedora de servicios esenciales de la mayor criticidad para el Estado y la sociedad.

Esquema Nacional de Seguridad

En la evolución de la ciberseguridad dentro de ENAIRE destacan diferentes momentos e hitos que marcan saltos cualitativos en términos de madurez y capacidad. Uno de ellos, como se ha indicado anteriormente, es sin duda la Certificación de Conformidad con el Esquema Nacional de Seguridad.

Más concretamente, se trata del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. En él se determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos, estableciendo los principios básicos y requisitos mínimos para una protección adecuada de la información. Asimismo, esta norma garantiza las condiciones necesarias de confianza en el uso de los medios electrónicos que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Posteriormente, con la entrada en vigor de la Ley 39/2015 y la Ley 40/2015, el alcance del ENS se amplía, aplicando a los Sistemas de Información del sector público para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Consiste, esencialmente, en un conjunto de principios básicos y requisitos mínimos que garantizan una protección adecuada de los servicios, sistemas, datos y comunicaciones, cuyo grado de rigurosidad y cumplimiento varía en función de la criticidad de los activos y sistemas de información analizados, valoración que en última instancia se refleja en la categorización de los mismos.

En este contexto, ENAIRE aborda en 2018 una primera certificación en Categoría Media, principalmente centrada en los Sistemas de Información de apoyo a la gestión empresarial. Se trata del primer contacto con una norma que, si bien es de obligado cumplimiento, en ese momento su extensión y aplicación aún no está generalizada. Gracias a esta primera adecuación se sientan las bases para construir un Sistema de Gestión de Seguridad de la Información, pilar básico sobre el cual se despliega y asienta toda la estructura procedimental de ciberseguridad de ENAIRE. Sirve, a su vez, como mecanismo de asimilación e interiorización de los principios y requisitos anteriormente referidos, lo que en última instancia supone un primer gran paso en términos organizativos y estructurales.

No obstante, el verdadero corazón de ENAIRE en términos operativos reside en la provisión de servicios de navegación aérea. Es esa su verdadera misión y, profundizando en esa primera línea trazada en 2018, en el año 2020 se produce un segundo logro que sin duda marca un antes y un después en la cronología de la ciberseguridad en ENAIRE: además de la renovación de la ya obtenida en 2018, se amplía y alcanza la Certificación de Conformidad con el Esquema Nacional de Seguridad en Categoría Alta en el ámbito de los sistemas operacionales críticos, directamente involucrados en la provisión de servicios de navegación aérea. Elementos como los sistemas de tratamiento y gestión de planes de vuelo, tráfico aéreo, comunicaciones, navegación, vigilancia, meteorología, información aeronáutica, supervisión y explotación técnica quedan bajo el paraguas de esta nueva certificación, la más completa y exigente en la materia.

Además de todos los beneficios que reporta la adecuación y satisfacción de una norma de estas características, esta certificación lleva aparejada para ENAIRE un valor añadido singular. Somos el primer Operador Crítico y de Servicios Esenciales de España en obtenerla, hecho que sin duda supone todo un hito en nuestro constante compromiso por alcanzar y mantener el más alto nivel de seguridad en todas nuestras operaciones.

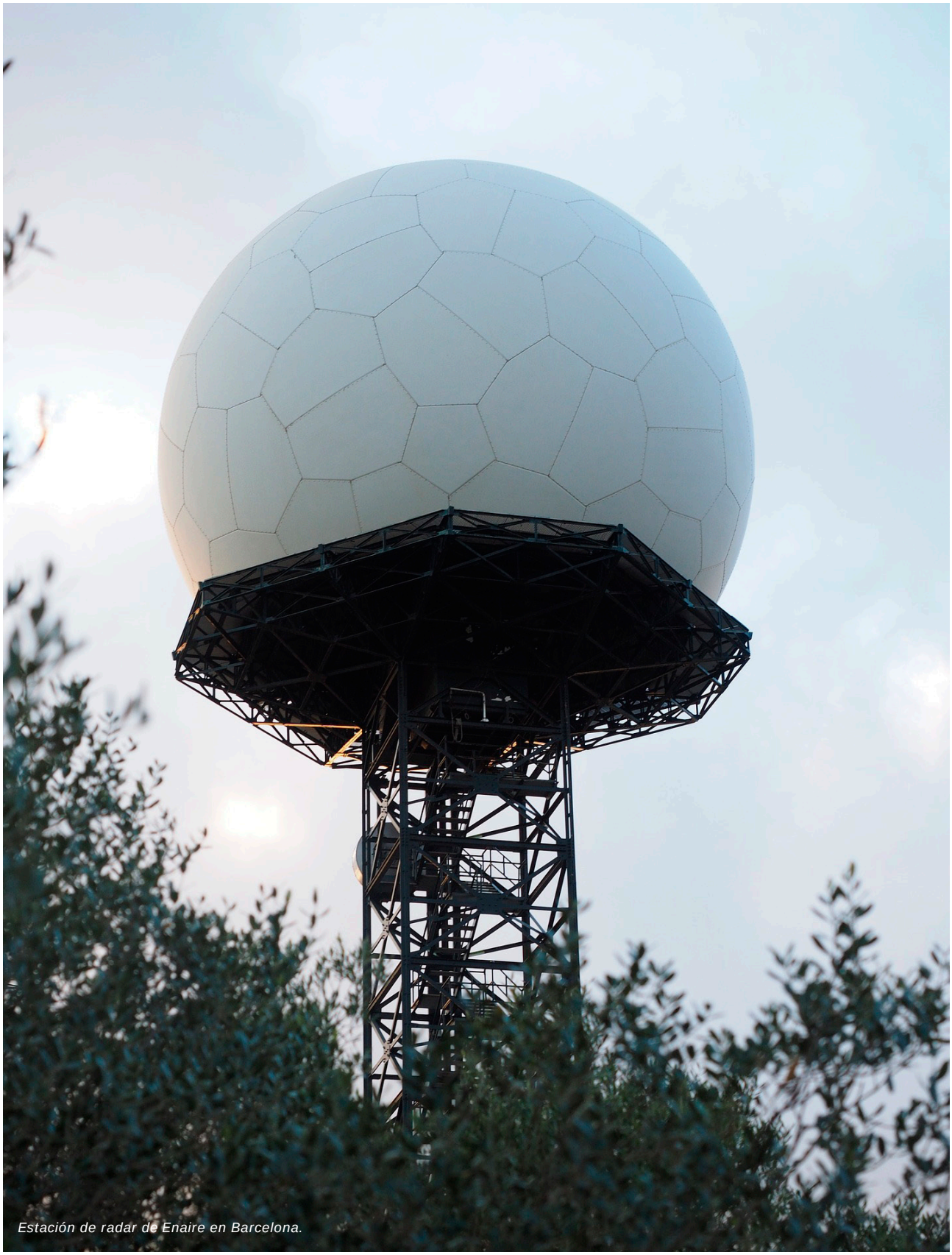
Este importante éxito sitúa a ENAIRE como un claro referente a la vanguardia de la ciberseguridad, gracias al gran esfuerzo y la activa participación de multitud de unidades técnicas de diferentes direcciones, tanto

ENAIRE en las IV Jornadas STIC del CCN-CERT

Bajo el lema “Nuevos retos, mismo compromiso”, las XIV Jornadas STIC CCN-CERT se celebraron en Madrid desde el 30 de noviembre hasta el 4 de diciembre de 2020 y congregaron a más de 115 ponentes de reconocido prestigio y 3.600 profesionales inscritos en sus jornadas y talleres.

La inauguración, retransmitida en abierto por el canal de YouTube del CCN-CERT, corrió a cargo de la secretaria de Estado y directora del Centro Nacional de Inteligencia, Paz Esteban. Asimismo, en el acto inaugural, participaron en una mesa redonda los principales actores de la ciberseguridad en España: Luis Jiménez, subdirector general del CCN; Rosa Díaz, directora de INCIBE; Francisco Javier Roca, 2º comandante del Mando Conjunto del Ciberespacio; Miguel Ángel Ballesteros, director del Departamento de Seguridad Nacional y Juan Carlos López Madera, jefe de la Oficina de Coordinación de Ciberseguridad.

En esta edición, celebrada online de manera excepcional como consecuencia de la covid-19, ENAIRE tuvo un papel protagonista. Con la ponencia “ENAIRE, primer operador de servicios esenciales conforme al Esquema Nacional de Seguridad en Categoría ALTA”, impartida de forma conjunta por Gerardo Sarmiento (jefe de la Oficina de Ciberseguridad de ENAIRE) y Miguel Ángel Lubián (Instituto CÍES), tuvimos la ocasión de compartir los aspectos clave que han permitido a ENAIRE ser pioneros en la consecución de la certificación de conformidad con el ENS en Categoría Alta, así como los principales retos afrontados y soluciones aplicadas, muchos de ellos comunes a otros operadores de servicios esenciales.



Estación de radar de Enaire en Barcelona.

en Servicios Centrales como en direcciones regionales. Adicionalmente, cabe destacar que, con la consecución de esta certificación, queda plenamente satisfecha toda la normativa de ciberseguridad en el sector de la aviación a escala europea, lo que posiciona igualmente a ENAIRE como uno de los más avanzados en este ámbito en el plano internacional.

Proveedores externos y cadena de suministro

Tal y como se ha expuesto anteriormente, en virtud de los principios y objetivos de la Política de Seguridad de la Información y de la certificación en el ENS, ENAIRE asume la obligación de cumplir los requisitos impuestos por el RD 3/2010 y las Instrucciones Técnicas de Seguridad (ITS) desarrolladas.

En este sentido, la Resolución de 13 de octubre de 2016 hace extensivo el cumplimiento de los compromisos de seguridad de la información a los proveedores adjudicatarios de los suministros y/o servicios externos.

Dicho con otras palabras, la seguridad de la información y la ciberseguridad son elementos de naturaleza transversal, en cuya satisfacción intervienen multitud de eslabones que, en última instancia, confieren robustez a toda la cadena. Esto no puede circunscribirse únicamente al propio personal o actividades de ENAIRE, sino que debe abarcar todo el ciclo de vida de cualquier producto o servicio, desde su concepción hasta su puesta en operación.

Por todo ello, otro elemento fundamental en ENAIRE es su relación con los proveedores externos y la cadena de suministro de productos y servicios. La seguridad, en su sentido más amplio, no debe entenderse como un requisito opcional o prescindible en ninguna de las actividades desarrolladas. Muy al contrario, se trata de un gen que debe estar presente desde la más temprana fase del diseño, contemplarse en cada una de las etapas del desarrollo y promoverse durante todo el ciclo de vida, abarcando -llegado el caso- incluso el desmantelamiento y retirada del servicio de cada uno de los elementos que componen el Sistema de Navegación Aérea.

En este aspecto, ENAIRE tiene muy presente en todos sus procesos de contratación externa esta circunstancia, exigiendo y trasladando a los potenciales oferentes los requisitos aplicables, adecuados y proporcionados, en función de la naturaleza y alcance de dicha contratación.

El factor humano

Para la consecución de todos los objetivos propuestos, además de las herramientas, equipamiento y recursos necesarios, un elemento singularmente relevante para ENAIRE es el factor humano, las personas. Nada de lo anterior es viable si no cuenta con el respaldo de un equipo multidisciplinar experto, altamente cualificado y actualizado, capaz de ejecutar las tareas encomendadas de forma ágil y eficaz.

La entidad protege los medios y servicios del sector de los ciberataques garantizando la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de su información aeronáutica

Esta consideración es, de hecho, aplicable a toda la plantilla de ENAIRE. Iniciativas como la formación, concienciación y sensibilización son claves en la consecución y mantenimiento de los más altos niveles de seguridad. En última instancia, por encima de cuestiones técnicas y más allá de complejas arquitecturas tecnológicas, el pilar fundamental sobre el que se cimienta la seguridad, ya sea operacional, física o ciberseguridad, es sencillo y elemental: la colaboración y participación de todos.

ENAIRE tiene muy presente este principio y lo aborda, además, tratando de acercar el lado más humano y amable de la ciberseguridad a cada una de las personas que componen su plantilla, procurando que se sientan reflejadas en sus actividades cotidianas, tanto profesionales como domésticas, de modo que puedan asimilar fácilmente los contenidos e interiorizar mejor las recomendaciones.

Si hay algo que diferencia a la ciberseguridad frente a otras

Impacto de la covid-19

La reciente crisis sanitaria ha supuesto, sin ninguna duda, un antes y un después en multitud de aspectos. La seguridad de la información, como no podía ser de otra manera, también se ha visto afectada de manera muy directa, adquiriendo un protagonismo especialmente destacado que, si bien ya disfrutaba, se ha consolidado al más alto nivel.

En el ámbito de la gestión, ENAIRE ha impulsado fórmulas alternativas mediante las cuales continuar prestando sus servicios, fiel a sus compromisos de seguridad, calidad y eficiencia. Ha sido en este contexto en el que los viejos paradigmas de trabajo presencial se han visto reemplazados por nuevas fórmulas, más flexibles y acordes a las circunstancias. Así, el teletrabajo ha recibido un fuerte impulso que lo ha situado en primera línea social y laboral. La infraestructura de comunicación y acceso remoto, ya existente y plenamente funcional, así como diferentes herramientas colaborativas, han visto incrementado su uso de manera exponencial. Todo ello se ha realizado, como es lógico, aplicando rigurosas medidas de seguridad con las que garantizar la integridad y confidencialidad de la información, así como la disponibilidad de los servicios asociados.

Las perspectivas a corto y medio plazo apuntan a que estas nuevas fórmulas de trabajo remoto han llegado para quedarse. Se ha puesto de manifiesto que los condicionantes que hasta la fecha habían contenido su despegue definitivo no eran técnicos, sino meramente organizativos y culturales. En última instancia, desde el punto de vista más constructivo y positivo, las crisis son también oportunidades en las que crecer y evolucionar en todos los ámbitos, superando los límites establecidos.

En este nuevo escenario, la ciberseguridad es y será un pilar fundamental sobre el que se sustentarán las organizaciones en la consolidación de un nuevo paradigma caracterizado por la flexibilidad y productividad que demanda esa “nueva normalidad” hacia la que nos dirigimos, tanto en el plano social como normativo y laboral.

áreas es que, dada su presencia y relevancia en nuestras propias vidas, resulta indisociable la vertiente personal de la profesional. Ello es así no porque convivan tecnologías o sistemas, sino por el factor común que une todos los puntos: el usuario. Si hasta ahora ya teníamos una estrecha relación con las nuevas tecnologías, en este nuevo escenario de teletrabajo la dependencia tecnológica es total. Los atacantes, plenamente conscientes de ello, han intensificado sus actividades, al haber crecido notablemente sus posibilidades de éxito por ese gran incremento en su uso.

En este contexto, la ciberseguridad adquiere un papel protagonista tanto en el ámbito profesional como en el personal: videollamadas, compras por internet, bulos, estafas bancarias, suplantación de identidad… No se trata de algo que se circunscriba a un horario laboral o a una actividad concreta. Por el contrario, abarca toda nuestra vida digital, de ahí la necesidad de difundir conocimiento e interiorizar buenas prácticas a título personal.

Por todo ello, en ENAIRE se dedica un gran esfuerzo en promover cualquier iniciativa que redunde en una mayor y mejor formación, concienciación y sensibilización de toda la plantilla. En este sentido, elabora cursos de ciberseguridad, difunde alertas y noticias, publica artículos, mantiene un portal web específico con novedades y recomendaciones, desarrolla iniciativas gamificadas e interactivas, así como valora y promueve cualquier actividad divulgativa que revierta en una mejor capacitación de todos.

Evolución

El comportamiento del entorno tecnológico, así como de la ciberseguridad, está intrínsecamente caracterizado por una constante evolución y reinvención, por lo que los próximos años se prevé que sean de gran actividad en el sector.

El proceso de transformación digital, en el cual está sumida la sociedad en su conjunto y ENAIRE en particular, propicia una creciente e inevitable dependencia de las TIC. Las nuevas y cada vez más complejas tecnologías llevan aparejadas la aparición de amenazas, igualmente innovadoras y disruptivas, que exigen la adaptación a estos nuevos retos, garantizando la adecuada

protección de la información y los servicios prestados.

El marco normativo que regula este nuevo escenario también está evolucionando. Las nuevas leyes, reglamentos y estándares están en constante actualización, tratando de satisfacer las demandas de la sociedad del modo más ágil posible.

Asimismo, todos los actores que intervienen en este progreso, conscientes de la criticidad del mismo, deben desarrollar sinergias y estrategias de colaboración, tanto a escala nacional como global, que les permitan hacer un frente común ante las contingencias derivadas de este estado de permanente cambio.

La evolución prevista a corto y medio plazo abunda en este planteamiento. La presencia de la tecnología en todos los ámbitos de actividad será cada día más patente. La interrelación e interconexión global de todos los sistemas, además de incrementar exponencialmente su rendimiento y eficiencia, conllevará nuevos riesgos, lo que conducirá a nuevas estrategias y tácticas que permitan su mitigación. La regulación será una tónica habitual una vez se alcance un punto de madurez adecuado, así como la coordinación de todos los implicados y la colaboración permanente en todos los ámbitos.

Sobre esa base, asumiendo cierto grado de incertidumbre por la propia naturaleza del entorno, es sobre la que ENAIRE cimienta su estrategia a través de la cual avanzar con firmeza y determinación hacia la consecución de sus objetivos.

Conclusión

A la luz de todo lo anterior, la ciberseguridad resulta manifiestamente prioritaria. Se debe promover y garantizar que se alcancen y mantengan las propiedades de seguridad de los activos tecnológicos de la organización y los usuarios contra los riesgos descritos. Para lograrlo, es imprescindible disponer de un conjunto de herramientas, políticas, salvaguardas, métodos de gestión de riesgos, acciones, inversiones, formación, buenas prácticas y tecnologías.

En definitiva, se deben acometer tareas de análisis, implantación y seguimiento que conduzcan a mitigar estos nuevos riesgos y amenazas. Es vital la asignación de recursos económicos, técnicos y humanos, así como adecuar las estructuras organizativas y procedimentales vinculadas a su gestión.

Sintetizando los principales conceptos presentados, cabría destacar tres líneas de actuación básicas a partir de las cuales trabajar en la consolidación y promoción de la ciberseguridad.

En primera instancia, su asentamiento en términos funcionales y operativos está fuertemente ligado al marco procedimental, directamente vinculado con el necesario cumplimiento normativo y la visión integral de la seguridad de la información.

Un segundo elemento indispensable es, como no puede ser de otra manera, el apartado tecnológico. La inversión, implementación y adecuada explotación de las herramientas necesarias resulta evidente, dada la naturaleza eminentemente técnica de esta materia.

No obstante, como nexo de unión de todo lo anterior, no debe olvidarse en ningún momento el punto neurálgico de la ciberseguridad: las personas. Toda inversión y despliegue de herramientas, cualesquiera que estas sean, debe estar siempre orientada y gestionada por y para los usuarios. Como ocurre siempre que hablamos de seguridad, el éxito de toda iniciativa en este ámbito está íntimamente ligado a la implicación y colaboración de todos. Más allá de costosas inversiones o complejos desarrollos, siempre termina sobresaliendo el mismo principio fundamental que la cimienta: la seguridad es cosa de todos. ■

La navegación aérea exige una monitorización permanente en materia de ciberseguridad.