Doc 9855
AN/459

Orientación sobre la utilización de la Internet pública para aplicaciones aeronáuticas

Aprobado por el Secretario General
y publicado bajo su responsabilidad

Primera edición — 2005

Organización de Aviación Civil Internacional

Publicado por separado en español, árabe, chino, francés, inglés y ruso, por la Organización de Aviación Civil Internacional. Toda la correspondencia, con excepción de los pedidos y suscripciones, debe dirigirse al Secretario General.

Los pedidos deben dirigirse a las direcciones siguientes junto con la correspondiente remesa (mediante giro bancario, cheque u orden de pago) en dólares estadounidenses o en la moneda del país de compra. En la Sede de la OACI también se aceptan pedidos pagaderos con tarjetas de crédito (American Express, MasterCard o Visa).

International Civil Aviation Organization. Attention: Document Sales Unit, 999 University Street, Montréal, Quebec, Canada H3C 5H7
Teléfono: +1 (514) 954-8022; Facsímile: +1 (514) 954-6769; Sitatex: YULCAYA; Correo-e: sales@icao.int; World Wide Web: http://www.icao.int

Alemania. UNO-Verlag GmbH, Am Hofgarten 10, D-53113 Bonn
Teléfono: +49 (0) 2 28-9 49 0 20; Facsímile: +49 (0) 2 28-9 49 02 22; Correo-e: info@uno-verlag.de; World Wide Web: http://www.uno-verlag.de

Camerún. KnowHow, 1, Rue de la Chambre de Commerce-Bonanjo, B.P. 4676, Douala, Teléfono: +237 343 98 42, Facsímile: + 237 343 89 25,
Correo-e: knowhow_doc@yahoo.fr

China. Glory Master International Limited, Room 434B, Hongshen Trade Centre, 428 Dong Fang Road, Pudong, Shangai 200120
Teléfono: +86 137 0177 4638; Facsímile: +86 21 5888 1629; Correo-e: glorymaster@online.sh.cn

Egipto. ICAO Regional Director, Middle East Office, Egyptian Civil Aviation Complex, Cairo Airport Road, Heliopolis, Cairo 11776
Teléfono: +20 (2) 267 4840; Facsímile: +20 (2) 267 4843; Sitatex: CAICAYA; Correo-e: icao@idsc.net.eg

Eslovaquia. Air Traffic Services of the Slovak Republic, Letové prevádzkové sluzby Slovenskej Republiky, State Enterprise, Letisko M.R. Stefánika,
823 07 Bratislava 21 / Teléfono: +421 (7) 4857 1111; Facsímile: +421 (7) 4857 2105

España. A.E.N.A. — Aeropuertos Españoles y Navegación Aérea, Calle Juan Ignacio Luca de Tena, 14, Planta Tercera, Despacho 3. 11,
28027 Madrid / Teléfono: +34 (91) 321-3148; Facsímile: +34 (91) 321-3157; Correo-e: sscc.ventasoaci@aena.es

Federación de Rusia. Aviaizdat, 48, Ivan Franko Street, Moscow 121351 / Teléfono: +7 (095) 417-0405; Facsímile: +7 (095) 417-0254

Francia. Directeur régional de l'OACI, Bureau Europe et Atlantique Nord, 3 bis, villa Émile-Bergerat, 92522 Neuilly-sur-Seine (Cedex)
Teléfono: +33 (1) 46 41 85 85; Facsímile: +33 (1) 46 41 85 00; Sitatex: PAREUYA; Correo-e: icaoeurnat@paris.icao.int

India. Oxford Book and Stationery Co., Scindia House, New Delhi 110001 *o* 17 Park Street, Calcutta 700016
Teléfono: +91 (11) 331-5896; Facsímile: +91 (11) 51514284

India. Sterling Book House — SBH, 181, Dr. D. N. Road, Fort, Bombay 400001
Teléfono: +91 (22) 2261 2521, 2265 9599; Facsímile: +91 (22) 2262 3551; Correo-e: sbh@vsnl.com

Japón. Japan Civil Aviation Promotion Foundation, 15-12, 1-chome, Toranomon, Minato-Ku, Tokyo
Teléfono: +81 (3) 3503-2686; Facsímile: +81 (3) 3503-2689

Kenya. ICAO Regional Director, Eastern and Southern African Office, United Nations Accommodation, P.O. Box 46294, Nairobi
Teléfono: +254 (20) 622 395; Facsímile: +254 (20) 623 028; Sitatex: NBOCAYA; Correo-e: icao@icao.unon.org

México. Director Regional de la OACI, Oficina Norteamérica, Centroamérica y Caribe, Av. Presidente Masaryk No. 29, 3er. Piso,
Col. Chapultepec Morales, C.P. 11570, México, D.F.
Teléfono: +52 (55) 52 50 32 11; Facsímile: +52 (55) 52 03 27 57; Correo-e: icao_nacc@mexico.icao.int

Nigeria. Landover Company, P.O. Box 3165, Ikeja, Lagos
Teléfono: +234 (1) 4979780; Facsímile: +234 (1) 4979788; Sitatex: LOSLORK; Correo-e: aviation@landovercompany.com

Perú. Director Regional de la OACI, Oficina Sudamérica, Apartado 4127, Lima 100
Teléfono: +51 (1) 575 1646; Facsímile: +51 (1) 575 0974; Sitatex: LIMCAYA; Correo-e: mail@lima.icao.int

Reino Unido. Airplan Flight Equipment Ltd. (AFE), 1a Ringway Trading Estate, Shadowmoss Road, Manchester M22 5LH
Teléfono: +44 161 499 0023; Facsímile: +44 161 499 0298 Correo-e: enquiries@afeonline.com; World Wide Web: http://www.afeonline.com

Senegal. Directeur régional de l'OACI, Bureau Afrique occidentale et centrale, Boîte postale 2356, Dakar
Teléfono: +221 839 9393; Facsímile: +221 823 6926; Sitatex: DKRCAYA; Correo-e: icaodkr@icao.sn

Sudáfrica. Avex Air Training (Pty) Ltd., Private Bag X102, Halfway House, 1685, Johannesburg
Teléfono: +27 (11) 315-0003/4; Facsímile: +27 (11) 805-3649; Correo-e: avex@iafrica.com

Suiza. Adeco-Editions van Diermen, Attn: Mr. Martin Richard Van Diermen, Chemin du Lacuez 41, CH-1807 Blonay
Teléfono: +41 021 943 2673; Facsímile: +41 021 943 3605; Correo-e: mvandiermen@adeco.org

Tailandia. ICAO Regional Director, Asia and Pacific Office, P.O. Box 11, Samyaek Ladprao, Bangkok 10901
Teléfono: +66 (2) 537 8189; Facsímile: +66 (2) 537 8199; Sitatex: BKKCAYA; Correo-e: icao_apac@bangkok.icao.int

6/05

Catálogo de publicaciones y ayudas audiovisuales de la OACI

Este catálogo anual comprende los títulos de todas las publicaciones y ayudas audiovisuales disponibles. En suplementos mensuales se anuncian las nuevas publicaciones y ayudas audiovisuales, enmiendas, suplementos, reimpresiones, etc.

Puede obtenerse gratuitamente pidiéndolo a la Subsección de venta de documentos, OACI.

Doc 9855
AN/459

Orientación sobre la utilización de la Internet pública para aplicaciones aeronáuticas

Aprobado por el Secretario General
y publicado bajo su responsabilidad

Primera edición — 2005

Organización de Aviación Civil Internacional

ENMIENDAS

La publicación de enmiendas y corrigendos se anuncia periódicamente en la *Revista de la OACI* y en los suplementos mensuales del *Catálogo de publicaciones y ayudas audiovisuales de la OACI*, documentos que deberían consultar quienes utilizan esta publicación. Las casillas en blanco facilitan la anotación.

REGISTRO DE ENMIENDAS Y CORRIGENDOS

ENMIENDAS			
Núm.	Fecha de aplicación	Fecha de anotación	Anotada por

CORRIGENDOS			
Núm.	Fecha de publicación	Fecha de anotación	Anotado por

PREÁMBULO

Este documento se ha creado con la colaboración del Grupo de estudio sobre el uso aeronáutico de la Internet pública (AUPISG) para ayudar a los Estados a hacer frente al uso cada vez mayor de la Internet pública (de aquí en adelante denominada “la Internet”) para determinadas aplicaciones aeronáuticas.

En este documento figuran orientaciones sobre la utilización de la Internet como medio de comunicación para aplicaciones aeronáuticas tierra-tierra en las que el tiempo no es primordial. La expresión “en las que el tiempo no es primordial” significa que la información que se va a transferir por intermedio de la Internet no tiene efectos inmediatos sobre un vuelo en curso. También se pone cierto énfasis en el material que podría ayudar a los Estados en el reconocimiento de proveedores de información aeronáutica por vía de la Internet.

Se abrigan esperanzas de que al seguir las orientaciones que figuran en este documento se eviten o reduzcan al mínimo las posibilidades de que los Estados y organizaciones internacionales adopten procedimientos no compatibles o divergentes al utilizar la Internet para determinadas aplicaciones operacionales.

El propósito de estas orientaciones es proporcionar las mejores prácticas de alto nivel, en vez de especificaciones técnicas detalladas, que se basan en procedimientos operacionales demostrados y productos estándar disponibles en el mercado (COTS). Cuando se incluyen ejemplos, se debe saber que es posible que se conviertan rápidamente en obsoletos como consecuencia de la velocidad de los cambios en la tecnología de Internet. Se recomienda que en el momento de la aplicación se utilice la solución más adecuada. Además, las orientaciones no abarcan los servicios que normalmente se proporcionan por medio de infraestructuras de comunicaciones especializadas, como las líneas arrendadas o las Intranet, que pueden utilizar tecnologías basadas en la Internet.

En el documento figuran algunos antecedentes históricos, consideraciones generales relativas a todos los servicios aeronáuticos basados en la Internet y consideraciones en relación con tipos específicos de servicios.

Por último, se debe tener en cuenta que en este documento no figura una declaración de la opinión de la OACI con respecto al lugar y el momento en que se debe o no utilizar la Internet para aplicaciones aeronáuticas. Si lo considera necesario, la OACI podrá elaborar una opinión al respecto, en una etapa ulterior.

ÍNDICE

GLOSARIO

Nota.— A continuación figuran explicaciones con el fin de facilitar la comprensión de los términos en el contexto en que se usan en este documento.

Ataques por denegación de servicio (DoS) [Denial of service (DoS) attacks]. Intentos de inundar un sitio o servidor de Internet. El resultado del ataque es que los verdaderos usuarios compiten por los mismos recursos que el atacante. Esta acción da como resultado que los verdaderos usuarios queden bloqueados o que toda la infraestructura se detenga. Los ataques por DoS distribuidos (DDoS) se coordinan desde muchas ubicaciones diferentes y pueden ser mucho más difíciles de manejar. Los atacantes utilizan a menudo un DoS como estrategia de desviación para disimular los esfuerzos para entrar en un sistema.

Autenticación sólida (Strong authentication). Método de autenticación de dos factores que se basa en algo que conoce el usuario (p. ej., contraseña/PIN) y algo que posee el usuario (p. ej., un código simbólico de autenticación). Las credenciales a dos niveles proporcionan una autenticación mucho más fiable de los usuarios. Véase RSA SecurID.

Certificado digital (Digital certificate). Medio electrónico de establecer credenciales de usuario para realizar negocios u otras transacciones en la web. Una autoridad de certificación (AC) emite el certificado. En él figuran el nombre del usuario, un número de serie, fechas de vencimiento, una copia de la clave pública del titular del certificado (que se utiliza para cifrar y descifrar los mensajes y firmas digitales), y la firma digital de la autoridad que emitió el certificado para que el receptor pueda verificar que es verdadero. Algunos certificados digitales se emiten de conformidad con la Recomendación X.509 de la Sección de Normalización de las Telecom.-nicaciones de la Unión Internacional de Telecomunicaciones. Los certificados digitales se pueden mantener en registros para que los usuarios autorizados puedan ver las claves públicas de los otros usuarios.

Correo electrónico (correo-e) [Electronic mail (email)]. Uno de los protocolos estándar de la Internet que permite que personas con diferentes computadoras y sistemas operativos se comuniquen entre sí. El correo electrónico permite enviar correspondencia individual o a varios receptores. El servidor de correo de una organización o un proveedor de servicios de Internet reciben el mensaje y lo retienen hasta que el destinatario inicia una sesión para recuperarlo.

Cortafuegos (Firewall). Dispositivo que protege los recursos de una red privada de usuarios provenientes de otras redes. Fundamentalmente, un cortafuegos en estrecha colaboración con un encaminador, filtra todos los paquetes de una red antes de decidir si lo transmite hacia su destino. Por lo general, el cortafuegos se instala fuera del resto de la red, de manera que las solicitudes de entrada no pasen directamente a los recursos de red privada.

Encaminador (Router). Dispositivo que determina el próximo punto de la red hacia el que se debe enviar un paquete de datos en ruta hacia su destino. El encaminador está conectado como mínimo a dos redes y determina por qué camino enviar cada paquete de datos basándose en la comprensión del estado de las redes a las que está conectado. Los encaminadores crean o mantienen una lista de las rutas disponibles y utilizan esa información para determinar la mejor ruta para un determinado paquete de datos.

Evaluación de riesgos (Risk assessment). Evaluación de las amenazas a un sistema, la posibilidad de que se aprovechen dichos riesgos y los efectos que puedan producir.

Extranet (Extranet). Red que complementa una Intranet cerrada por medio del suministro de acceso a clientes, proveedores, subcontratistas y otras personas externas a la organización que necesitan información selectiva de la misma. No se tiene acceso desde la Internet general.

Hipermedia (Hypermedia). Es similar al hipertexto, pero incluye otros elementos multimedia interenlazados, como gráficos, sonido y vídeo.

Hipertexto (Hypertext). Forma de texto que incluye enlaces visibles a otras páginas de textos o medios, al que se accede pulsando con el ratón sobre el enlace o seleccionándolo.

Infraestructura de clave pública (PKI) [Public key infrastructure (PKI)]. Sistema de certificados digitales, autoridades de certificación y otras autoridades de registro que verifican y autentican la validez de cada parte que interviene en una transacción de Internet. Las PKI están en evolución y no existe una sola PKI, ni siquiera un estándar único acordado para establecer una PKI.

Internet (Internet). Sistema de redes de computadoras con interconexión a nivel mundial y que utilizan el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) para la transmisión y recuperación de la información.

Intranet (Intranet). Red privada dentro de una organización que utiliza el TCP/IP para transmitir y recuperar información. Los sitios dentro de una Intranet generalmente están cerrados a la Internet y pueden acceder a ellos solamente los miembros de esa organización.

Lenguaje ampliable de composición (XML) [Extensible Markup Language (XML)]. Un paso en la evolución de los formatos de datos para la web (posterior a HTML).

Lenguaje de composición de hipertexto (HTML) [Hypertext Markup Language (HTML)]. Sistema de codificación que se utiliza para crear páginas en la World Wide Web (WWW). Una página escrita en HTML es un archivo de texto en el que se incluyen etiquetas en corchetes que controlan los tipos y tamaños de letras, la inserción de gráficos, la diagramación de cuadros y marcos, los párrafos, llamadas a programas que se deben iniciar próximamente, y enlaces en hipertexto a otras páginas.

Localizador uniforme de recursos (URL) [Uniform Resource Locator (URL)]. Designador de la ubicación de un recurso en la Internet. Se puede escribir en la ventana de ubicación del navegador para conectarse con la dirección deseada (p. ej., un sitio web).

Matriz redundante de discos independientes (RAID) (originalmente denominada matriz redundante de discos económicos) [Redundant array of independent disks (RAID)]. Método de almacenar los mismos datos en diferentes lugares (por esa razón se denomina redundante) de manera que las operaciones de entrada/salida se puedan superponer de manera equilibrada, mejorando el rendimiento. La redundancia aumenta el tiempo medio entre fallos (MTBF) y por lo tanto aumenta también la tolerancia a fallos. Para el sistema operativo una RAID funciona como un disco duro lógico único.

Navegador (Browser). Soporte lógico que carga y hace la presentación de una página web. El navegador interpreta los códigos HTML o XML (véase más abajo) de los archivos de la página web, ejecuta las órdenes escritas y programas incluidos, cuando es necesario proporciona los medios de cifrado y descifrado para seguridad, presenta gráficos (excepto los navegadores solamente de texto), reproduce música y vídeos y proporciona enlaces a páginas relacionadas.

Nivel de conectores seguros (SSL) [Secure Sockets Layer (SSL)]. Método de cifrado de comunicaciones en la Internet. El SSL garantiza que la información se envía, sin modificaciones, solamente al receptor previsto. En los lugares de compra o servicios bancarios en línea se utiliza frecuentemente tecnología SSL para proteger la información sobre tarjetas de crédito y otro tipo de información delicada.

Protocolo de control de transmisión (TCP) [Transmission Control Protocol (TCP)]. Protocolo de comunicaciones (utilizado en la Internet) que proporciona servicios de comunicaciones fiables, huésped a huésped, en una red de conmutación de paquetes o una interconexión de tales redes.

Protocolo de Internet (IP) [Internet protocol (IP)]. Protocolo que se utiliza para encaminar paquetes de datos desde la fuente al destino en un entorno Internet (redes interconectadas).

Protocolo de transferencia de hipertexto (seguro) [Hypertext Transport Protocol (Secure) (https)]. El mecanismo de cifrado de comunicaciones estándar en la World Wide Web. Es el HTTP que funciona en el nivel de conectores seguros (SSL).

Proveedores de servicios aeronáuticos por Internet (IASP) [Internet aviation service provider (IASP)]. Empresa reconocida que proporciona información aeronáutica utilizando la Internet como medio de comunicación.

Proveedor de servicios de Internet (ISP) [Internet service provider (ISP)]. Empresa que proporciona acceso a Internet y una infraestructura de comunicaciones.

Puerto (Port). Dirección interna definida previamente que sirve como vía desde la aplicación al nivel de transporte (TCP) o en sentido inverso.

Red privada virtual (VPN) [Virtual private network (VPN)]. Red que utiliza un "túnel" autenticado y seguro a través de una red pública (p. ej., la Internet). Los puntos finales del túnel VPN están autenticados y normalmente utilizan autenticación sólida. Los contenidos se aíslan de la red pública utilizando el cifrado.

RSA (RSA). Sistema de cifrado y autenticación en Internet que utiliza un algoritmo creado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. El sistema es de propiedad de la empresa RSA Security que otorga licencias de tecnologías de algoritmo.

SecurID (SecurID). RSA SecurID® es un mecanismo de "autenticación sólida" en el que son necesarios un código simbólico y un número de identificación personal (PIN).

Servidor (Server). Computadora o dispositivo en una red que distribuye o administra recursos de la red. Por ejemplo, un servidor de archivos es una computadora y dispositivo de almacenamiento dedicado a almacenar archivos. Cualquier usuario de la red puede almacenar archivos en el servidor. Un servidor de impresora es una computadora que administra una o más impresoras, y un servidor de red es una computadora que gestiona el tráfico de la red. Un servidor de base de datos es un sistema de computadoras que procesa solicitudes a la base de datos. Los servidores a menudo están especializados, lo que quiere decir que no realizan otras tareas además de las tareas de servidor. Sin embargo, en sistemas operativos de multi-procesamiento, una computadora puede ejecutar varios programas a la vez. En este caso, se puede denominar servidor al programa que está gestionando los recursos en vez de a la computadora completa.

Sistema operativo (OS) integrado [Operating system (OS) integrated]. Característica o función incluida en el sistema operativo de la computadora (p. ej., Internet Explorer en Windows).

Sitio web (Website). Una o más páginas web conectadas en el marco de un propietario, gestión o tema comunes.

World Wide Web (WWW) [World Wide Web (WWW)]. Protocolo de Internet que utiliza HTML, hipertexto e hipermedia para crear páginas con enlaces a otras páginas. Las páginas WWW pueden incluir gráficos, sonido, vídeo y texto.

Zona desmilitarizada (DMZ) [Demilitarized zone (DMZ)]. Una red establecida entre otras dos. No es parte de la red interna ni directamente parte de la Internet. La infraestructura de la zona tiene determinada protección contra ataques externos, pero se sigue considerando vulnerable.

Capítulo 1

ANTECEDENTES

1.1 La palabra “Internet” es una contracción de la expresión en inglés “interconnected network”, red interconectada. Sin embargo, a lo que se hace referencia comúnmente, que es el tema de este documento, la “Internet pública” (o simplemente “Internet”), es la colaboración internacional organizada libremente de redes interconectadas autónomas que utilizan el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) para la interconexión de redes. El término estrechamente relacionado “World Wide Web (WWW)” se refiere a la red mundial de servidores (con soporte lógico instalado en las computadoras que están conectadas a la Internet) que permite que se combinen y procesen juntos archivos con textos, gráficos, sonido y vídeo, y enlaces (conexiones activas a otros lugares o recursos de la web).

1.2 El origen de la Internet se remonta a los esfuerzos de investigación realizados en los Estados Unidos para establecer una red segura computadora-computadora a mediados de la década de los sesenta. Estos trabajos dieron como resultado la red del Organismo de proyectos de investigación avanzados (dependencia del Departamento de Defensa) (Red ARPA o ARPANET), que comenzó su funcionamiento conectando las computadoras de algunas universidades de los Estados Unidos en 1969. Aunque el primer correo electrónico fue intercambiado a través de ARPANET en 1972, muchos consideran que el 1 de enero de 1983 fue el comienzo “oficial” de la Internet. En esa fecha la red se conectó a través del conjunto de protocolos TCP/IP, que habían sido elaborados a mediados de los años setenta y aceptados por el Gobierno de los Estados Unidos en 1978. Gradualmente se fueron conectando otras redes a la ARPANET y comenzó a crecer la Internet. La ARPANET propiamente dicha dejó de existir en 1989, pero la Internet mantuvo su crecimiento explosivo debido al interés creciente y a la disponibilidad de poderosas computadoras personales, enlaces de comunicaciones como la fibra óptica y redes de área local/redes de área extensa. El control del tráfico en la Internet se traspasó al sector comercial en 1995.

1.3 Por lo general, los usuarios arriendan los servicios a proveedores de servicios de Internet (ISP) comerciales. La demanda en continuo crecimiento de servicios Internet, que se evidencia en el enorme aumento del número de usuarios (de 200 millones en 1998 a casi 500 millones a comienzos de 2002) proporciona un incentivo muy fuerte a los proveedores de servicios para que sigan mejorando la capacidad y el rendimiento de sus sistemas y ofrezcan mejores servicios competitivos. Por lo tanto, se puede concluir que, en general, donde se encuentren servicios Internet comerciales (y se permita la competencia) la probabilidad de encontrar un nivel de servicio apropiado aumenta con el tiempo.

1.4 Tradicionalmente, la comunidad de la aviación civil ha insistido en la posibilidad de tener sus propios sistemas de comunicaciones especializados, basándose en la fiabilidad, integridad, seguridad y su incidencia en la seguridad aeronáutica. Esto ha provocado cierta desgana de muchos integrantes del personal aeronáutico a la hora de formalizar el uso de la Internet, que no está bajo el control de ninguna autoridad aeronáutica. Sin embargo, a causa de su disponibilidad generalizada, facilidad de acceso (especialmente por el público), precio asequible, velocidad y facilidad de uso, algunos Estados han comenzado a utilizar la Internet para determinadas aplicaciones (p. ej., servicios de información meteorológica y aeronáutica). Además, en algunas regiones del mundo, en que los sistemas de comunicaciones aeronáuticas especializados son insuficientes o no se pueden justificar económicamente debido a los muy bajos niveles de tráfico, se está utilizando la Internet como medio de comunicaciones tierra-tierra.

1.5 La OACI utiliza ampliamente los servicios de Internet (principalmente el correo electrónico y el acceso a la web) para la distribución de información, documentos y comunicaciones administrativas. La facilidad de acceso y utilización y el alto nivel de integridad de esos servicios han mejorado en gran medida el proceso general de

comunicaciones de la Organización. Sin embargo, la Organización ha tratado con cautela la idea de utilizar la Internet para aplicaciones relacionadas con la seguridad. Esto se debe principalmente a que la Organización ha realizado grandes esfuerzos con miras a normalizar los sistemas de comunicaciones que pueden apoyar requisitos operacionales rigurosos en materia de seguridad aeronáutica y seguridad (protección) de la aviación, previendo que los Estados los implantarán de conformidad con los planes regionales de navegación aérea.

1.6 En la esfera de las comunicaciones tierra-tierra, la OACI ha creado el sistema de tratamiento de mensajes ATS (AMHS), un sistema moderno que forma parte del sector tierra-tierra de la red de telecomunicaciones aeronáuticas (ATN), para sustituir la antigua red de telecomunicaciones fijas aeronáuticas (AFTN). Al igual que la AFTN [y la red OACI común de intercambio de datos (CIDIN)], el AMHS es un sistema especializado que apoya aplicaciones de seguridad aeronáutica. Sin embargo, hasta el momento, el sistema se ha implantado solamente a escala muy limitada, y serán necesarios aún muchos años hasta que se pueda utilizar un verdadero sistema de intercambio de mensajes aeronáuticos a nivel mundial. Por el momento, ha surgido la Internet como medio popular que puede servir en las necesidades de intercambio de mensajes de la comunidad aeronáutica. Además, a diferencia de la AFTN, la CIDIN y el AMHS, que son redes cerradas, es decir limitadas a usuarios autorizados relacionados con la aviación, la Internet está abierta al público general y por lo tanto permite que los pilotos u otros usuarios actuales o posibles de información aeronáutica tengan acceso a los bancos de datos e interactúen con las autoridades aeronáuticas pertinentes, según sea necesario, desde el hogar o cualquier otro lugar en que exista una conexión apropiada. Por lo tanto, la Internet constituye un buen complemento de la forma en que se realizan actualmente las comunicaciones aeronáuticas.

1.7 Tomando nota de lo anterior y como respuesta a las recomendaciones de grupos regionales de planificación y ejecución y, más recientemente, de la Reunión departamental de meteorología (MET) (2002), la OACI inició estudios sobre la utilización de la Internet pública para todas las categorías de aplicaciones aeronáuticas (aunque solamente en el contexto de comunicaciones tierra-tierra), dando la debida consideración a la fiabilidad, integridad, facilidad de acceso y consideraciones relativas a la seguridad (protección). Las directivas que figuran en este documento son los primeros resultados de dichos estudios.

1.8 En este documento figuran orientaciones sobre la utilización de la Internet para aplicaciones aeronáuticas tierra-tierra en las que el tiempo no es primordial. Generalmente dichas aplicaciones incluyen la distribución y el intercambio de información entre:

a) una autoridad estatal y usuarios (dentro del Estado);

b) dos o más autoridades estatales; o

c) un tercero (por lo general una entidad comercial) y usuarios (en el mismo Estado o no).

1.9 Se debe garantizar a los usuarios de información aeronáutica que lo que están utilizando ha sido proporcionado por una fuente aprobada por el Estado, se gestiona de manera adecuada y se comunica con integridad. Esta cuestión es más compleja si la información se transmite a través de la Internet. En este caso participan dos procesos de acreditación, uno para las fuentes de información aeronáutica y el otro para el suministro por la Internet de la información aeronáutica. Las orientaciones que figuran en este documento se centran principalmente en el suministro de información aeronáutica por la Internet.

Capítulo 2

RESPONSABILIDAD DE LOS ESTADOS

2.1 GENERALIDADES

2.1.1 Por lo general, la utilización de la Internet como medio para proporcionar o intercambiar información operacional no exime a los Estados de sus obligaciones y responsabilidades respecto a la implantación de un servicio fijo aeronáutico (AFS) y otras instalaciones y servicios que se han establecido por acuerdo regional y documentado en los planes regionales de navegación aérea de la OACI.

2.1.2 Además, como cualquier otra instalación o servicio, la utilización de la Internet para el intercambio de datos y mensajes entre Estados debería estar sujeta a acuerdos bilaterales, multilaterales o regionales y debería quedar adecuadamente reflejada en los planes regionales de navegación aérea.

2.1.3 Los Estados que permiten la utilización de la Internet deberían:

a) acreditar los órganos [de aquí en adelante denominados proveedores de servicios aeronáuticos por Internet (IASP)] que proporcionarán el suministro o intercambio de información basado en Internet; y

b) garantizar que cuentan con tecnología de la información y conocimientos especializados de seguridad de la información adecuados para supervisar el proceso de acreditación descrito a continuación.

2.1.4 Para los fines de acreditación y supervisión de los IASP, los Estados deberían:

a) publicar y mantener una lista de los IASP acreditados, con detalles de los servicios que se han acreditado y las fechas de vencimiento de la acreditación;

b) exigir que los IASP asesoren a los usuarios de cualquier limitación relacionada con la provisión de sus servicios. Además, el IASP debería declarar cuáles son los servicios de contingencia o alternativa. Por ejemplo, en el caso de falla de un sistema de Internet en el momento de presentar un plan de vuelo, el usuario debería llamar a los servicios de tránsito aéreo o instalación de servicios de vuelo y presentar la información por medios convencionales;

c) exigir que los IASP reduzcan, utilizando interfaces de usuario bien diseñadas, la posibilidad de que se transmita accidentalmente información incorrecta y proporcionen la capacitación adecuada a los usuarios; y

d) volver a acreditar a un IASP tras un intervalo de como mínimo tres años o cuando el IASP introduzca cambios importantes en su organización o infraestructura.

2.2 DISPOSICIONES APLICABLES DE LA OACI

2.2.1 En el Capítulo 3 del Anexo 15 — *Servicios de información aeronáutica,* se especifican las responsabilidades de los Estados con respecto al suministro de información aeronáutica y las funciones de un servicio de información aeronáutica. Se incluyen disposiciones relativas al establecimiento de un sistema de

calidad, intercambio de información aeronáutica, derechos de autor, etc. Los principios fundamentales del Anexo 15, que provienen del Artículo 28 del Convenio sobre Aviación Civil Internacional, consisten en que cada Estado es responsable de poner a disposición toda la información pertinente y necesaria para la operación de aeronaves afectadas a la aviación civil internacional dentro de su territorio, así como en zonas fuera de su territorio en las que el Estado es responsable de los servicios de tránsito aéreo.

2.2.2 Se debe observar en particular la Sección 3.1 del Anexo 15, en la que se dispone que el Estado interesado seguirá siendo el responsable de la información publicada tanto si suministra servicios de información aeronáutica, comparte el suministro de los servicios con otro Estado o delega la autoridad para el suministro del servicio en una entidad extragubernamental. En consecuencia, cuando los Estados utilizan la Internet como medio complementario para publicar su información aeronáutica deberían asegurarse de que existen procesos y procedimientos de sistema de calidad adecuados para prestar apoyo a la información suministrada bajo su responsabilidad y además deberían acreditar los sitios de Internet que publican tal información.

2.2.3 En el Anexo 3 — *Servicio meteorológico para la navegación aérea internacional*, Capítulo 2, 2.2, se especifican las responsabilidades de los Estados con respecto al suministro, garantía de calidad y utilización de información meteorológica.

2.2.4 En el Anexo 4 — *Cartas aeronáuticas*, Capítulo 1, 1.3, se especifican las responsabilidades de los Estados con respecto a la disponibilidad de cartas aeronáuticas, y en el Capítulo 2, 2.17, se proporcionan los requisitos para la gestión de calidad de los datos aeronáuticos de las cartas.

2.3 ACREDITACIÓN DE UN IASP

2.3.1 La acreditación de un IASP es diferente a la de las fuentes de información aeronáutica. La acreditación de fuentes de datos, inclusive la recolección, presentación y oportunidad de los datos es un requisito previo a la acreditación de un IASP y no entra en el ámbito de aplicación de este documento.

2.3.2 Para garantizar que la información que se proporciona a través de la Internet cumple con las mejores prácticas actuales relativas a confidencialidad, integridad, autenticidad y disponibilidad, es necesario que los Estados elaboren procedimientos de acreditación para los IASP que distribuyan información y servicios a través de la Internet. En los siguientes párrafos se proporcionan orientaciones a tal efecto.

2.3.3 Sería conveniente que los Estados exigieran que los IASP siguieran las medidas de alto nivel que se presentan en la Figura 2-1. Cada Estado en particular puede tomar medidas adicionales.

2.3.4 En los siguientes párrafos se describen los elementos básicos de la acreditación típica que se presenta en la Figura 2-1.

Plan de servicios

2.3.5 Los IASP deben proporcionar una descripción de los servicios de Internet que van a brindar. En la descripción se debería indicar:

a) el tipo de servicio(s). Los servicios típicos incluyen, entre otros, servicios de información aeronáutica (AIS), MET, comunicaciones tipo AFTN y presentación de planes de vuelo;

b) la región en que se aplicará (p. ej., local, regional o mundial); y

c) el mercado al que va destinado (es decir, aviación general, aviación de negocios, aviación comercial).

El plan de servicios es un requisito previo para el proceso de gestión de riesgos.

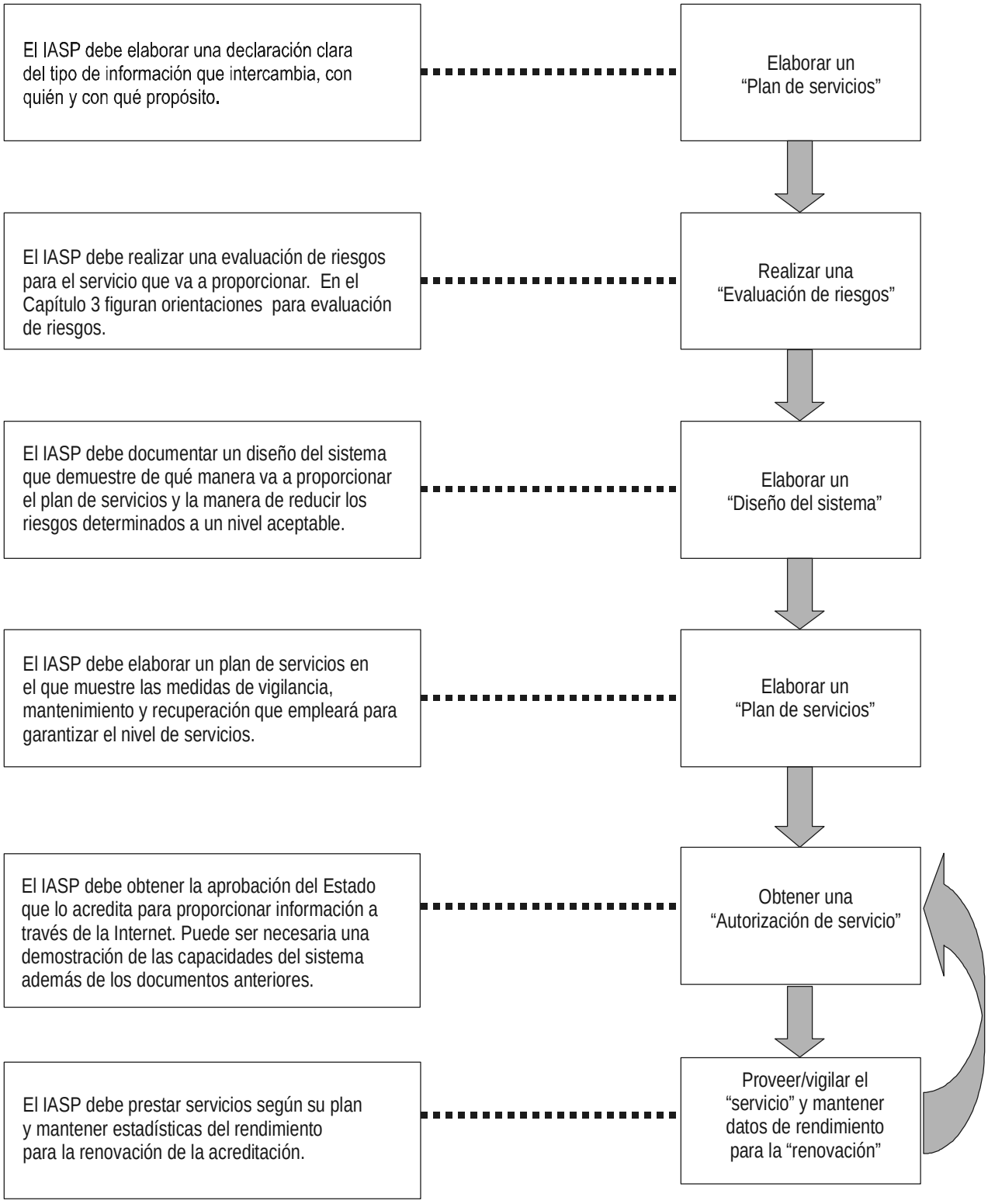

Figura 2-1. Proceso típico para la evaluación de un IASP

Evaluación de riesgos

2.3.6 Después de haber elaborado un plan de servicios, será necesario que el IASP estudie los riesgos que se presentan al ofrecer este servicio en la Internet. En el Capítulo 3 figuran orientaciones sobre evaluación de riesgos.

Diseño del sistema

2.3.7 Después de haber identificado los riesgos del servicio, el IASP diseñará su sistema para reducir estos riesgos a un nivel aceptable para el servicio que prevé suministrar. En el Capítulo 3 figuran orientaciones sobre estrategias para reducción de riesgos.

Planificación en servicio

2.3.8 Después de haber concluido el plan de servicios, la evaluación de riesgos y el diseño del sistema, será necesario que el IASP analice la manera en que mantendrá el servicio al nivel necesario de calidad.

Mantenimiento del sistema

2.3.9 Es necesario que el IASP tenga un plan de mantenimiento que permita la operación continua del sistema en armonía con el tipo de servicio que ofrece a los usuarios aeronáuticos. En el plan se debería incluir el mantenimiento preventivo regular tanto del soporte físico como del soporte lógico. Deberán tener primordial importancia las actualizaciones regulares del soporte lógico de seguridad. Además, es necesario que el IASP determine los repuestos del soporte físico que mantendrá para permitir que se cumplan los requisitos del "tiempo de reparación" declarado. Se deberían determinar los niveles de capacitación mínimos para el personal de mantenimiento.

Acuerdo de servicios con el proveedor de servicios de Internet (ISP)

2.3.10 El IASP debería concertar un acuerdo de nivel de servicios con su ISP, en el que se especifiquen los requisitos de disponibilidad de servicios, inclusive los tiempos de reparación, informes sobre fallas, puntos de contacto de transferencia ascendente e informes de rendimiento mensuales.

Archivo de datos y de transacciones

2.3.11 Es necesario que el IASP actúe de conformidad con los requisitos de gestión de datos que figuran en los Anexos de la OACI para los servicios que ofrece. Entre ellos se incluye el mantenimiento de registros de los datos que se ofrecen en todo momento y registro de transacciones para demostrar los datos que se han suministrado a usuarios determinados.

Nota.— En los casos en que se mantienen registros de aplicación, red o acceso, el Estado determinará el período durante el que se deben conservar. Por lo general, se considera adecuado conservar los mensajes AFTN durante 30 días civiles (como figura en el Anexo 10 — Telecomunicaciones aeronáuticas*, Volumen II —* Procedimientos de comunicaciones*, incluso los que tienen categoría de PANS). Sin embargo, en el caso de recibir la notificación de un accidente, incidente o aeronave retrasada, o a solicitud del Estado, los IASP deberían conservar los datos relativos a ese suceso de manera indefinida o hasta el momento en que la ley autorice la destrucción de los datos. Los IASP deben poner a disposición esos datos en forma de copia legible, certificable y fiel a solicitud del Estado.*

Interrupción del sistema planificada o no planificada

2.3.12 Es necesario que el IASP cuente con un plan de gestión de interrupciones de servicio.

Recuperación de desastres (fallas catastróficas)

2.3.13 Es necesario que el IASP tenga un plan de recuperación en caso de desastres (fallas catastróficas), cuya magnitud dependerá del tipo de servicios que ofrezca.

Vigilancia del sistema operacional

2.3.14 El IASP deberá elaborar una serie de criterios y objetivos del rendimiento que permitirán a la autoridad de acreditación del Estado determinar si se cumplen los objetivos de rendimiento del servicio.

Concesión de autorización de servicio

2.3.15 La autoridad de acreditación del Estado deberá evaluar los procesos de diseño del sistema del IASP y la planificación durante el servicio para determinar si el IASP puede ejecutar su plan de servicios y si se han puesto en práctica estrategias para reducir los riesgos identificados en la evaluación de riesgos a un nivel aceptable.

2.3.16 Antes de la primera acreditación, los Estados podrían exigir una demostración del servicio que se ofrecerá en la Internet para asegurarse de que el sistema cumple con los criterios de rendimiento.

2.3.17 Además, los Estados podrían considerar la posibilidad de pedir al IASP que una empresa adecuada de evaluación de la seguridad de la tecnología de la información ensaye el sistema a fondo. El ensayo debería comprender “pruebas de penetración”, puertos y servicios de exploración y las pruebas necesarias para garantizar que se han instalado las últimas actualizaciones y “parches” de seguridad en el sistema operativo y los programas (inclusive los antivirus).

2.3.18 Los Estados deberían otorgar la acreditación para que un IASP ofrezca su plan de servicios durante un período fijo de tiempo (p. ej., uno o dos años). Cuando un IASP solicita la renovación de su acreditación, debería aportar datos históricos que demuestren su rendimiento.

2.3.19 La acreditación no debería ser transferible y el IASP debería aclararlo cuando esté en conexión con otros proveedores de sitios web. Un IASP debería indicar claramente qué Estado le ha dado la acreditación para suministrar información aeronáutica a través de la Internet y el tipo de información que puede proporcionar con su acreditación (de acuerdo con el plan de servicios que ha presentado a la autoridad de acreditación del Estado).

2.3.20 De conformidad con las disposiciones actuales de la OACI, la acreditación se aplica solamente a la provisión de servicios a usuarios que los utilizan en o desde el Estado de acreditación. Los Estados pueden acordar arreglos recíprocos de acreditación.

Vigilancia y suministro de servicios

2.3.21 El IASP debería vigilar de manera activa el rendimiento de los servicios de Internet. Los criterios de rendimiento determinados en el plan durante el servicio se deberán vigilar con una frecuencia que permita corregir rápidamente el rendimiento insuficiente. El IASP debería mantener registros completos de la vigilancia del rendimiento. La autoridad de acreditación del Estado podría hacer auditorías de estos registros durante el período de acreditación del servicio y se deberían presentar cuando el IASP hace una solicitud de renovación de la acreditación.

2.3.22 El IASP debería incluir enlaces en su sitio web que permitan mantener el intercambio de información entre los usuarios aeronáuticos y el IASP.

2.3.23 El IASP debería incluir un enlace acordado con la autoridad de acreditación del Estado que permita a los usuarios aeronáuticos comprobar si tiene o no acreditación y mantener un intercambio de información o comentarios directamente con la autoridad de acreditación del Estado.

2.4 IMPOSICIÓN DE DERECHOS

2.4.1 Los Estados incurren en gastos importantes al suministrar información aeronáutica o meteorológica. En una amplia mayoría de Estados, estos gastos se recuperan mediante la recaudación de derechos por servicios de navegación aérea a los usuarios. Sin embargo, con el desarrollo de la tecnología de la información moderna y en el contexto de la comercialización que existe actualmente, los usuarios finales tienen la opción de obtener dichos productos del Estado correspondiente o de un tercer proveedor comercial.

2.4.2 Por lo tanto, puede haber ocasiones en que organismos comerciales o Estados intenten obtener información aeronáutica y otro tipo de documentos de navegación aérea del Estado originador. En tales casos, este Estado puede optar por concertar un acuerdo individual con la parte interesada relativo a las condiciones y costos, si existen, que se aplicarán al suministro de tal información para su consiguiente reedición. Sin embargo, se debe observar que en el Anexo 15 se prevé el intercambio de información aeronáutica, sin cargo alguno, entre los Estados contratantes de la OACI.

2.4.3 En general, los esquemas de imposición de derechos para la recuperación de los costos se deben establecer de conformidad con los principios que figuran en el Doc 9082 — *Políticas de la OACI sobre derechos aeroportuarios y por servicios de navegación aérea*.

2.5 INDICADORES DE RENDIMIENTO

El Estado debería considerar la posibilidad de establecer indicadores de rendimiento obligatorios para cada servicio, según sea adecuado. Estos indicadores de rendimiento se centrarían en los clientes y se podrían establecer en consulta con comunidades de usuarios. En general, sería deseable que en la lista de indicadores de rendimiento se incluyeran los siguientes:

a) ***Disponibilidad.*** En cualquier mes civil, podrá no haber acceso al servicio durante un período mínimo especificado, y ninguna interrupción individual de servicio será superior a otro período especificado. En esto se incluyen interrupciones para mantenimiento planificado. Claro está que los períodos especificados variarán según el tipo de servicio que se proporcione.

b) ***Accesibilidad.*** La velocidad de impresión de las páginas que proporcione el servicio a los usuarios no será inferior a un valor específico. Se podría introducir una segunda medida si los usuarios necesitan descargar archivos de datos de gran volumen.

Nota.— Aunque los indicadores de rendimiento se establecen a juicio del Estado, deberían mantenerse dentro de límites razonables. Además, el Estado debería adherirse a una política coherente entre los proveedores en que se prevea que los servicios similares se realizan en general con criterios similares.

2.6 PROPIEDAD INTELECTUAL

2.6.1 Aunque en la mayor parte de los Estados aún se está analizando la cuestión de los derechos de autor en línea, se puede suponer que los contenidos ya protegidos por las leyes nacionales de un Estado quedan igualmente protegidos en la Internet. Aunque los textos que un Estado pone a disposición en la Internet probablemente tienen derecho a estar protegidos de igual manera que los textos en copia impresa, al publicar textos en la Internet existen mayores riesgos de violación de los derechos de autor. Lo más probable es que se cometa una infracción copiando la totalidad o una parte importante de un trabajo con derechos de autor sin el consentimiento del Estado.

2.6.2 Es posible que algunos Estados prefieran asegurar el cumplimiento de sus derechos de autor para determinada información (en forma escrita, electrónica o como carta visual). En consecuencia, estos Estados podrían preferir utilizar sus derechos para negar el permiso a alguna parte a copiar y volver a publicar tales textos. Los Estados que deseen facilitar la difusión de sus textos pueden optar por insistir, de conformidad con sus obligaciones con la OACI y la legislación nacional, en que se adopten los procedimientos adecuados de control de calidad y auditoría por parte de un tercero como condición para otorgar una licencia para copiar o volver a publicar información aeronáutica.

2.6.3 La manera más eficaz de informar a los usuarios con respecto a la propiedad intelectual al publicar en la Internet es asegurarse de que el IASP exhibe de manera visible un aviso sobre derechos de autor © en su sitio web, en el que se expone claramente lo que puede hacer o no el usuario con los textos protegidos e iniciar acciones jurídicas en el caso de infracciones. En el apéndice de este capítulo figura un ejemplo de aviso sobre derechos de autor de un Estado.

2.6.4 Otra posibilidad de reducir al mínimo los riesgos de violación de los derechos de autor es utilizar soporte lógico de protección de copia o gestión de derechos digitales, como la marca de agua digital.

— — — — — — — — —

Apéndice del Capítulo 2

EJEMPLO DE AVISO SOBRE DERECHOS DE AUTOR

Nota.— El aviso sobre derechos de autor siguiente se utiliza en Australia para un sitio basado en Internet en el que figuran datos estáticos AIS. Se reproduce gracias a la amable autorización de Airservices Australia.

Todos los textos y publicaciones del servicio de información aeronáutica de Airservices Australia ("AIS Publications") están sujetos a derechos de autor. Se incluyen específicamente todos los elementos de la documentación integrada de información aeronáutica ("IAIP"). A menos que se especifique de otra manera, sólo podrá utilizar las publicaciones AIS si se descargan, presentan o imprimen (en la forma sin variaciones que incluye este aviso) con fines informativos. En los fines informativos se cuenta la utilización operacional pero, con excepción de lo indicado en el permiso anterior y en virtud de la Ley de derechos de autor de 1968, ninguna parte de las publicaciones AIS se puede reproducir, almacenar en un sistema de recuperación, transmitir, redistribuir, reeditar o utilizar comercialmente de ninguna manera sin el permiso previo por escrito de Airservices Australia. Si desea hacer uso de cualquier parte de las publicaciones AIS de alguna manera no autorizada en este aviso, comuníquese con las publicaciones de Airservices Australia para solicitar una licencia.

Capítulo 3

CONSIDERACIONES TÉCNICAS

3.1 CLASIFICACIÓN DE LOS MENSAJES SEGÚN CATEGORÍAS

3.1.1 El conjunto de protocolos de Internet garantiza la integridad de los mensajes que se transmiten en circunstancias normales. Sin embargo, en su condición de medio público, la Internet está expuesta a determinados ataques contra la seguridad (p. ej., denegación de servicio o virus en la computadora) que pueden disminuir gravemente la capacidad o aún detener temporalmente el funcionamiento útil.

3.1.2 Se pueden emplear programas de seguridad de la información para garantizar la autenticidad, integridad o confidencialidad de los mensajes. Sin embargo, estas medidas no pueden contrarrestar la congestión en la red (debido al elevado tráfico en algunos momentos o al atascamiento malintencionado). Como tal, la utilización de la Internet para operaciones aeronáuticas se debería limitar al intercambio de mensajes, información o datos para los que el tiempo no es primordial. En el contexto de este documento, la expresión “el tiempo no es primordial” significa que lo que se está comunicando no tiene efectos inmediatos sobre un vuelo en curso.

3.1.3 Sin embargo, es necesario aclarar exactamente qué categorías de mensajes aeronáuticos cumplen con el criterio mencionado de que el tiempo no es primordial. De conformidad con las categorías de mensajes y sus indicadores de prioridad (para transmitir vía AFTN) que figuran en el Anexo 10, Volumen II, se considerará que el tiempo no es primordial en las siguientes categorías de mensajes y, por lo tanto, podrían transmitirse a través de la Internet:

a) determinados mensajes MET (véase el Capítulo 4 de este manual);

b) mensajes sobre la regularidad de los vuelos;

c) determinados mensajes AIS (véase el Capítulo 5 de este manual);

d) planes de vuelo y mensajes correspondientes (véase el Capítulo 5 de este manual);

e) mensajes administrativos; y

f) mensajes de servicios (cuando corresponda).

3.1.5 Sin perjuicio de lo que antecede, determinados tipos de mensajes, en que se considera que el tiempo es primordial para aeronaves en vuelo, se pueden catalogar como que no lo son si se utilizan en un contexto previo al vuelo. En los Capítulos 4 y 5 figuran más detalles sobre mensajes MET y AIS, respectivamente, en los que el tiempo no se considera primordial.

3.1.6 En los casos en que se ponen a disposición datos en que el tiempo es primordial, para fines informativos solamente, se debe avisar a los usuarios que dichos datos se deben obtener por los medios adecuados si se piensa utilizarlos en un contexto en que el tiempo es primordial (p. ej., en caso de avisos a una aeronave en vuelo).

3.2 CONTENIDO

3.2.1 Al preparar sus servicios, un IASP debe tener en cuenta el texto que figura en los siguientes párrafos.

3.2.2 Se debe aclarar a los usuarios el tipo de información que se pone a disposición por medio del servicio. Por ejemplo, es necesario que los usuarios sepan concretamente qué información se pone a disposición a través del servicio para garantizarles que tendrían todo el contenido necesario para sus operaciones.

3.2.3 Los servicios acreditados para proporcionar información meteorológica deberían, como mínimo, poner a disposición el conjunto completo de los productos del Anexo 3 (*Servicio meteorológico para la navegación aérea internacional*) que suministra el Estado pertenecientes a la categoría en que el tiempo no es primordial para la seguridad durante el vuelo o la preparación previa al vuelo.

3.2.4 Se deben señalar claramente al usuario las fuentes de información que utiliza el servicio acreditado.

3.2.5 Se debe presentar claramente a los usuarios del servicio la validez de la información proporcionada.

3.2.6 La información de carácter histórico, no operacional o no acreditada se debe marcar claramente como tal si se pone a disposición en el mismo servicio como información operacional, es decir, información que ha caducado, información archivada.

Nota.— La información no acreditada puede incluir información o servicios de valor añadido que estén en elaboración o versiones previas a su distribución.

3.2.7 Se deberían poner a disposición del usuario procedimientos que expliquen la mejor manera de utilizar los servicios acreditados.

3.3 EVALUACIÓN Y GESTIÓN DE RIESGOS

3.3.1 Como parte del proceso de acreditación que se define anteriormente, es necesario que un IASP mantenga procesos de evaluación y gestión de riesgos para el servicio que se propone proporcionar.

3.3.2 La evaluación y reducción de riesgos exige que se realicen análisis del entorno del sistema en sus aspectos físico, lógico, sistemático y de procedimientos.

3.3.3 Con el fin de gestionar los riesgos correspondientes al suministro de servicios aeronáuticos basados en la Internet, es necesario comprender de qué riesgos se trata. Esto se realiza en el proceso de evaluación de riesgos. Una vez que se han determinado los riesgos se pueden tomar las medidas necesarias para garantizar que se controlan a un nivel aceptable (es decir, un nivel aceptable para el IASP y el Estado de acreditación).

3.3.4 Las orientaciones que se presentan en esta sección tienen el propósito de complementar el proceso normalizado de gestión de riesgos y de tratar las cuestiones específicas a la tecnología de la información.

3.3.5 En la norma ISO/IEC 17799:2000, *Tecnología de información — Código de práctica para la gestión de la seguridad de la información* figura más información pertinente a esta sección.

3.3.6 En la publicación *Secrets and Lies, Digital Security in a Networked World*. (Secretos y mentiras, Seguridad digital en un mundo de redes interconectadas), de Bruce Schneier (John Wiley & Sons, Inc., 2004; ISBN: 0-471-45380-3), figura más información sobre este tema para un público no técnico.

3.4 PROCESO DE EVALUACIÓN DE RIESGOS

3.4.1 Con el fin de realizar una evaluación de riesgos, se deben seguir los siguientes pasos:

a) determinar qué elementos del activo están amenazados y su valor; en algunos casos el resultado de esta evaluación se denomina declaración de sensibilidad;

b) determinar la sensibilidad de dichos elementos del activo;

c) determinar las amenazas a dichos elementos del activo;

d) determinar las fuentes de la amenaza;

e) determinar o estimar la probabilidad de que dichas amenazas puedan hacerse realidad y afectar a los elementos del activo;

f) determinar las repercusiones, si los elementos del activo fueran afectados;

g) de las repercusiones y la probabilidad de que se produzcan se deriva el riesgo para los elementos del activo;

h) decidir las medidas necesarias para reducir el riesgo si éste no es aceptable (p. ej., medidas de seguridad, tanto técnicas como de procedimiento); e

i) volver a evaluar el riesgo teniendo en cuenta las medidas de reducción, y determinar si éstas tuvieron éxito o fueron suficientes.

3.4.2 El proceso de evaluación de riesgos se debería repetir a la luz de cada estrategia de reducción que se utilice, hasta que se considere que el riesgo es aceptable. Además, el proceso de evaluación y gestión de riesgos se debería continuar durante la vida útil operacional del servicio. También es importante tener en cuenta que la medida de reducción necesaria será proporcional al valor de los elementos del activo que se esté protegiendo. Cada amenaza se debería describir bajo los títulos de: “amenaza”, “fuente de amenaza”, “probabilidad (de materializarse)”, “repercusiones” y, por último, “riesgo”.

Identificación de los elementos del activo amenazados

3.4.3 Antes de que se pueda considerar la posibilidad de tomar medidas de seguridad adecuadas, es primordial comprender exactamente qué se está protegiendo. En todos los sistemas se tendrá en cuenta:

a) el sistema mismo, incluido el equipo y aplicaciones físicas;

b) los datos del sistema; y

c) la reputación o imagen comercial de la organización.

3.4.4 Es esencial tener en cuenta las conexiones de red y el correspondiente flujo de datos que entran y salen del sistema. Cada sistema con enlace de prolongación tiene también riesgos y por esa razón son también necesarias más evaluaciones de riesgos para estos sistemas.

Determinación de la sensibilidad

3.4.5 Los siguientes factores son los puntos sensibles a diversos ataques en un sistema típico:

a) ***Confidencialidad.*** La sensibilidad de la información o de los elementos del activo a la divulgación no autorizada, registrada como clasificación o designación, cada una de las cuales implica un cierto grado de daño si se produce la divulgación no autorizada;

b) ***Integridad.*** La sensibilidad de la información o de los elementos del activo a la alteración o destrucción;

c) ***Disponibilidad.*** La sensibilidad de un servicio que proporciona información, o acceso a elementos del activo que no están disponibles para apoyar las funciones operativas; y

d) ***Autenticidad.*** La sensibilidad del servicio a un usuario no legítimo que pueda tener acceso a la información o a los elementos del activo.

Determinación de amenazas a los elementos del activo

3.4.6 Existen amenazas en relación con cada punto sensible, según se describe a continuación:

a) ***Interceptación: amenaza a la "confidencialidad"****.* Amenaza de una persona que logra el acceso no autorizado a la información. ¿Puede una persona acceder a información confidencial y que no está autorizado a ver (p. ej., por razones comerciales o legales)? También se deben tener en cuenta las amenazas a la información en tránsito.

b) ***Modificación: amenaza a la "integridad"****.* Es la amenaza de una persona que hace modificaciones fraudulentas en el sistema o los datos. Por ejemplo, si una persona puede introducir datos falsos para que un pronóstico sea inexacto. Si el sistema puede entrar por sí mismo en una forma de funcionamiento que arroje resultados erróneos. Si se pueden modificar los datos mientras se encuentran en la plataforma del IASP. Si se puede comprometer la integridad de los datos mientras están en tránsito desde una fuente acreditada al IASP; del IASP al usuario; del usuario al IASP (p. ej., AFTN, presentación de un plan de vuelo, entrada de datos de observación meteorológica). ¿Es posible detectar algunas de estas modificaciones fraudulentas?

c) ***Interrupción: amenaza a la "disponibilidad".*** ¿Suministra el servicio las prestaciones apropiadas para la utilización operacional? ¿Se degrada la calidad del servicio en momentos de máxima demanda? ¿Se puede bloquear el uso de los elementos del activo? ¿Se puede impedir que usuarios legítimos presenten información inundando el servicio con entradas falsas [p. ej., ataques por denegación de servicio (DoS)]? El ejemplo más común es el caso en que los servidores de la web simplemente quedan sobrecargados de conexiones, de forma que los usuarios legítimos no pueden tener acceso al servicio.

d) ***Disfraz: amenaza a la "autenticidad".*** Esta amenaza se presenta cuando una persona se hace pasar por otra. Por ejemplo, en un servicio de Internet ¿se puede garantizar que los "clientes" que inician una sesión son en realidad quienes pretenden ser? (ya que existe la posibilidad de que algunas personas intenten obtener el servicio de forma gratuita). ¿Se puede verificar que quien intenta obtener acceso de administrador es en realidad un administrador legítimo? ¿Pueden verificar los usuarios que están en comunicación con el servicio "verdadero" y no un escenario presentado por un atacante? En la Internet puede ser especialmente difícil confirmar que en el otro extremo de la conexión se encuentra la persona o el lugar que afirma ser.

3.4.7 Las amenazas mencionadas suelen manifestarse de muchas maneras, algunas de las cuales se presentan a continuación:

a) ***Datos/información****.* No disponibilidad, interrupción (pérdida), interceptación, alteración, fabricación o destrucción;

b) ***Personas/personal****.* Omisión, error, negligencia, imprudencia, indolencia, sabotaje o falta de conocimientos;

c) ***Red (Intranet, Internet, etc.)****.* Acceso no autorizado, mantenimiento, falla o ataques a la seguridad (p. ej., interceptación, bromas, falsa identidad, violación de la integridad o denegación de servicio);

d) ***Soporte físico****.* Mantenimiento, fallas (inclusive del suministro de energía) o robo; y

e) ***Soporte lógico y sistema****.* Interrupción, modificaciones/parches o fallas.

Determinación de las fuentes de amenaza

3.4.8 La posibilidad de un ataque y sus repercusiones pueden depender de la fuente del ataque. Las amenazas se pueden dividir, además, en relación con las fuentes. La división más sencilla de las posibles fuentes de amenaza es:

a) personal (de plantilla);

b) personal (administradores);

c) consultores/contratistas;

d) competidores;

e) intrusos informáticos (hackers) (no cualificados pero numerosos);

f) intrusos informáticos (hackers) (minoría selecta, altamente cualificados);

g) entidades motivadas y organizadas políticamente; y

h) sucesos naturales.

Determinación de la probabilidad de que se materialice una amenaza

3.4.9 Esta parte de la evaluación de riesgos se vuelve subjetiva. Los dos factores que se deben tener en cuenta son:

a) ***La facilidad de realizar un ataque****.* Depende de las medidas de seguridad que se establezcan, el tipo de sistema instalado y la ubicación del sistema. Depende también del nivel de competencia de la fuente de amenaza y las oportunidades que tenga, así como de los recursos disponibles. Esto puede cambiar con el tiempo. Algunos ataques se pueden considerar muy teóricos y difíciles, pero si se elaboran las herramientas para su automatización se vuelven más fáciles de realizar.

b) ***Motivación de la fuente de amenazas****.* El mero hecho de que una persona pueda iniciar un ataque no significa que lo vaya a realizar. Por lo tanto, es importante comprender los motivos de las fuentes de amenazas.

3.4.10 Por ejemplo, en una organización moderna típica, la mayor parte del personal de plantilla no tiene acceso directo a su servidor web (es decir, el único acceso es a través de un navegador). Por lo tanto, aunque tuviera la motivación, sería relativamente difícil para la mayor parte del personal iniciar un ataque (especialmente si existe vigilancia). La situación del “administrador del sistema” es muy diferente. El administrador del sistema puede

provocar interrupciones graves, aunque de manera involuntaria, y prácticamente no existe ninguna defensa contra tales posibles ataques. Por lo tanto, se otorga un alto grado de confianza al administrador del sistema.

3.4.11 De manera similar, los intrusos informáticos sin cualificación están siempre tratando de atacar servidores web, siendo en gran parte su motivación la de poder jactarse de la cantidad de sistemas que han puesto a prueba. Si se mantiene y actualiza el soporte lógico del sistema los riesgos pueden ser bastante bajos. Sin embargo, es probable que los intrusos informáticos altamente cualificados tengan éxito al atacar casi cualquier servidor. La cuestión entonces es saber la razón por la que atacan específicamente una organización en particular.

3.4.12 Los sucesos naturales (es decir, incendios, terremotos, inundaciones o tornados), aunque son raros, afectarán al suministro de servicios y, por lo tanto, será necesario tenerlos también en cuenta en el proceso de gestión de riesgos.

Determinación de las repercusiones de una amenaza

3.4.13 Este es también un análisis subjetivo. El objetivo es responder (en la mayor medida posible) preguntas como:

a) ¿Cuánto costará recuperar los datos dañados?

b) ¿Cuál es el valor de estos datos?

c) ¿Qué le va a costar a la reputación de la organización?

d) ¿Cuáles son las sanciones contractuales?

e) ¿Qué repercusiones operacionales tiene en el usuario la pérdida o desaparición de información?

3.4.14 Las repercusiones o el nivel de gravedad se basarán en factores específicos del sistema que incluyen, sin que esta lista sea exhaustiva, la naturaleza de la amenaza, la capacidad funcional del sistema, sus interfaces con sistemas operativos, la criticidad de los datos suministrados, la continuidad de las actividades y el usuario de la información.

Evaluación del riesgo

3.4.15 Si las repercusiones y la probabilidad están registradas en el formulario estándar de gestión de riesgos (muy baja | baja | media | alta | extremadamente alta), el riesgo se puede calcular exactamente de la misma manera (es decir, como el producto de las repercusiones y probabilidades, donde las repercusiones son el efecto sobre el sistema/organización, y las probabilidades son la posibilidad de que la amenaza se materialice; a su vez ésta se deriva del tipo de amenaza y la fuente de amenaza, teniendo en cuenta tanto el nivel de competencia como la motivación.

Estrategias para reducir los riesgos

3.4.16 Es primordial emplear estrategias para reducir los riesgos cuando se toman en cuenta el valor del servicio o la gravedad de la falla del servicio. Por ejemplo, es probable que un IASP pequeño que suministre información previa al vuelo para la comunidad de la aviación general necesite medidas de reducción de riesgos mucho menos estrictas que un IASP que suministra presentación de planes de vuelo y servicios de exposición verbal previa al vuelo para empresas que explotan aeronaves comerciales. No obstante la relación entre el alcance de la estrategia de reducción y el valor del servicio, se deben adoptar siempre medidas razonables para preservar la integridad de los datos aeronáuticos.

3.4.17 Se debería observar que el factor más importante en la estrategia de reducción de riesgos es la gestión de parches de las aplicaciones de soporte lógico. Independientemente de lo bien que se haya diseñado e implantado el sistema, si el soporte lógico es obsoleto (es decir, no se han aplicado los últimos parches), el servicio será vulnerable a ataques.

3.4.18 Las estrategias de reducción de riesgos se agrupan de acuerdo con el punto sensible que protegen. A continuación se enumeran los principales puntos sensibles y las posibles medidas pertinentes para reducir los riesgos:

a) confidencialidad

1) permitir procesos que garanticen que los datos que tiene el proveedor de servicios se mantienen con carácter confidencial;

2) garantizar que el diseño del sistema, la arquitectura de la red y los procesos de gestión de la vida útil administran, a nivel aceptable, la probabilidad de violaciones de acceso;

3) gestionar, a nivel aceptable, la probabilidad de que se “roben” datos confidenciales en el tránsito entre el proveedor de servicios y el usuario, implantando el cifrado de datos, cuando sea necesario;

4) gestionar, a nivel aceptable, basándose en el nivel de gravedad, la probabilidad de que usuarios sin autorización o utilizando autorizaciones falsas puedan acceder al sitio;

5) implantar el uso de nombres de usuario y contraseñas u otros mecanismos de autenticación de usuarios, cuando sea necesario, basándose en el nivel de gravedad;

6) implantar los procesos de registro y validación de usuarios proporcionales al nivel de gravedad;

7) implantar políticas de responsabilidad del usuario, con términos y condiciones proporcionales al nivel de gravedad;

8) garantizar la gestión adecuada de las contraseñas; y

9) garantizar la eliminación segura del equipo.

b) integridad

Nota.— En el Anexo 15, Capítulo 3, 3.2.8, figuran los requisitos de integridad de los datos aeronáuticos como parte del sistema de calidad.

1) garantizar que los datos originales provienen de una fuente segura;

2) garantizar que la modificación o el nuevo formato de los datos originales no pone en peligro su integridad;

3) gestionar, a nivel aceptable, la probabilidad de que los datos se puedan modificar en el tránsito entre la fuente segura y el proveedor de servicios mediante:

i) la gestión, a nivel aceptable, de la probabilidad de que los datos que mantiene el proveedor de servicios puedan tener modificaciones fraudulentas;

ii) la gestión, a nivel aceptable, de la probabilidad de que los datos se puedan modificar en el tránsito entre el proveedor de servicios y el usuario;

iii) garantizar que en el caso de que los datos que mantiene el proveedor de servicios se corrompan, se pueden volver a restaurar datos “limpios”;

iv) la gestión, a nivel aceptable, de la probabilidad de que se pueda atacar el almacenamiento de datos a través del sitio web;

v) garantizar que se mantienen registros de las transacciones con el usuario, con la fecha y hora estampadas, con el fin de que no se puedan rechazar. (Debería ser posible reconstruir los productos a que el usuario tuvo acceso para verificar que los recibió, si los mismos productos no están archivados);

c) disponibilidad

1) aplicar un acuerdo del nivel de servicios con el ISP (y con todo tipo de apoyo de mantenimiento correspondiente) que garantice una disponibilidad adecuada a la importancia del sitio;

2) garantizar que el diseño del sistema tiene en cuenta una redundancia adecuada a la importancia del sitio;

3) garantizar que en el diseño del sistema, arquitectura de la red y procesos de gestión de la vida útil se controla, a nivel aceptable, la probabilidad de que se pueda inhabilitar la plataforma con mala intención (p. ej., intrusos informáticos, virus y gusanos informáticos, denegación de servicio, denegación distribuida de servicio o sucesos naturales como inundaciones);

4) garantizar que se controla, en el diseño del sistema, arquitectura de la red, gestión de la vida útil y procesos de capacitación, a nivel aceptable, la probabilidad de que se pueda inhabilitar la plataforma mediante actividades benévolas; y

5) aplicar un proceso de intercambio de información con los clientes para garantizar que se pueden determinar las cuestiones relativas al rendimiento y éstas pueden dirigirse al proveedor de servicios.

d) autenticidad

1) garantizar que el usuario puede verificar fácilmente que el proveedor ha sido acreditado (para el Estado en el que el usuario desea comenzar el viaje);

2) garantizar que el usuario puede verificar que el proveedor de servicios es quien declara ser; y

3) garantizar que, cuando sea necesario, el proveedor pueda verificar quién es el usuario.

3.4.17 Además, cuando sea necesario, el IASP debería estar en condiciones de comprobar que se entrega la información adecuada al usuario. Esta medida recibe el nombre de “no rechazo”.

3.4.18 Una vez que se ha concluido la evaluación inicial de riesgos, el proceso de gestión de riesgos debería entrar en una fase iterativa en la que se consideren medidas para la reducción de riesgos y se establezca una nueva evaluación de riesgos, hasta que el IASP (y el Estado de acreditación) determinen que los riesgos que permanezcan son aceptables. Además, durante la prestación del servicio aparecerán nuevos riesgos. El proceso de gestión de riesgos deberá tratarlos y volver a evaluar los riesgos existentes y nuevos teniendo en cuenta la información actualizada y las mejores prácticas.

3.4.19 En el apéndice de este capítulo se enumeran determinadas estrategias de gestión de amenazas y riesgos y se presentan en relación con las mejores prácticas actuales que se sugiere aplicar en un ambiente de tecnología de la información.

3.4.20 Además, según el Proyecto de seguridad en aplicaciones web abiertas [Open Web Application Security Project) (OWASP) (http://www.owasp.org)], en la página de *Las diez vulnerabilidades de seguridad más críticas en aplicaciones web*, actualizada en 2004, se define un cierto número de estrategias para combatir los puntos vulnerables en aplicaciones web.

— — — — — — — —

Apéndice del Capítulo 3

MEJORES PRÁCTICAS ACTUALES PARA ESTRATEGIAS DE REDUCCIÓN DE RIESGOS EN UN AMBIENTE DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

Nota.— Como los adelantos en la tecnología de Internet son frecuentes, las soluciones tecnológicas específicas que pueden figurar en la columna "mejores prácticas actuales" son ejemplos de lo que era actual en el momento de la publicación.

Estrategia para la reducción de riesgos	Categoría de sensibilidad	Mejores prácticas actuales	Se utiliza si la gravedad de las repercusiones es	
			Baja	Alta
Implantar una autenticación del usuario adecuada al nivel de amenaza	Autenticidad	• Acceso de usuario anónimo • Para iniciar una sesión son necesarios el nombre y contraseña del usuario • Se inicia la sesión con el nombre y contraseña del usuario, además de PIN para funciones específicas • Certificado digital (p. ej., SSL) • Protocolo de transferencia seguro (https) • RSA SecurID • VPN, OS-integrado • Soporte lógico para el cliente (autenticación por código simbólico)	✓ ✓	 ✓ ✓ ✓ ✓ ✓ ✓
Implantar un registro de usuario y procedimiento de validación adecuados al nivel de amenaza	Autenticidad	• Registro en línea sin validación • Registro en formulario impreso sin validación • Registro en línea con validación • Registro en formulario impreso con validación • Registro en línea con detalles de acceso enviados por otro canal (es decir, correo electrónico, correo) para ayudar a garantizar que el usuario registrado se puede identificar realmente	✓ ✓	 ✓ ✓ ✓
Aplicar términos y condiciones a los usuarios adecuados al nivel de amenaza	Autenticidad	• Mantener confidencialidad de contraseña; no compartir • Siempre finalizar la sesión del sitio • Comunicar al proveedor de servicios los cambios de la información pertinente	✓ ✓ ✓	
Aplicar un cifrado de datos adecuado al nivel de confidencialidad	Integridad	• HTTPS, SSL • PKI (y otros)	✓	 ✓
Gestionar, a nivel aceptable, la probabilidad de que se puedan modificar los datos durante el tránsito entre la fuente asegurada y el proveedor de servicios	Integridad	• Utilizar la Internet con cifrado y autenticación apropiados (HTTPS, SSL). • Utilizar una conexión privada segura o una red privada virtual (VPN) para obtener datos de la fuente asegurada. No utilizar la Internet pública sin una conexión VPN debidamente asegurada.	✓	 ✓

Estrategia para la reducción de riesgos	Categoría de sensibilidad	Mejores prácticas actuales	Se utiliza si la gravedad de las repercusiones es	
			Baja	Alta
Gestionar, a nivel aceptable, la probabilidad de que los datos que mantiene el proveedor de servicios puedan tener modificaciones fraudulentas Gestionar, a nivel aceptable, la probabilidad de que se puedan modificar los datos durante el tránsito entre el proveedor de servicios y el usuario Gestionar, a nivel aceptable, la probabilidad de que se pueda atacar el almacenamiento de datos a través del sitio web	Integridad	• Utilizar soporte lógico cortafuegos e infraestructura fortalecida; no permitir el acceso directo al almacenamiento de datos. • Emplear cortafuegos físicos, servidores proxy, sistemas host de protección contra intrusiones (HIPS) y sistemas de detección de intrusiones basados en la red (NIDS), según sea necesario. • Utilizar un doble nivel de cortafuegos, de diferentes fabricantes, para reducir la posibilidad de que la vulnerabilidad afecte al proveedor de servicios. • Verificar los certificados digitales del proveedor. • Evitar “intermediarios” y asegurarse de que los datos pasan directamente a los usuarios (se logrará con SSL). • Utilizar una infraestructura de cortafuego entre el servidor web y el servidor de aplicación (si existe) y el almacenamiento de datos además de límites externos para crear DMZ (zonas desmilitarizadas). • Utilizar varias DMZ para separar los componentes de funcionamiento (es decir, servidor web, servidor de aplicaciones, servidor de base de datos).	✓	 ✓ ✓ ✓ ✓ ✓ ✓
Asegurarse de que en el caso de corrupción de los datos que mantiene el proveedor de servicios se pueden restaurar datos “limpios” Garantizar que se mantienen los registros de las transacciones con el usuario, con su fecha y hora estampadas, para fines de no rechazo (debe estar en condiciones de reconstruir los productos a los que se tuvo realmente acceso para verificar lo que el usuario recibió en el caso de que no se archiven los productos)	Integridad	• Almacenar los registros en formatos interoperables, como ASCII. • Archivos de registros firmados digitalmente. • Garantizar que el sistema y las copias de datos de seguridad se controlan desde un dominio seguro. • Garantizar que las copias de seguridad se almacenan en un dominio seguro. • Mantener almacenamientos externos con fines de recuperación de archivos en caso de falla catastrófica.	✓	 ✓ ✓ ✓ ✓
Aplicar procedimientos de intercambio de información con los clientes para garantizar que se pueden determinar y tratar sus preocupaciones	Todas	• Mostrador de servicios al cliente con apoyo telefónico y sistema de rastreo de notificaciones de problemas. • Intercambio de información con los clientes por correo electrónico y sistema de rastreo de notificaciones de problemas.	 ✓	✓

Estrategia para la reducción de riesgos	Categoría de sensibilidad	Mejores prácticas actuales	Se utiliza si la gravedad de las repercusiones es	
			Baja	Alta
Garantizar que el usuario puede verificar fácilmente que el proveedor ha sido acreditado (para el Estado en el que el usuario desea iniciar el viaje) Garantizar que el usuario puede verificar que el proveedor de servicios es lo que declara ser Garantizar que, cuando sea necesario, el proveedor puede verificar quién es el usuario	Confidencialidad	• Verificación del usuario por medio de nombre y contraseña de usuario. • Verificación del usuario utilizando certificados digitales de cliente. • Verificación del proveedor utilizando certificados digitales. • Exhibir en lugar destacado en el sitio un logotipo oficial en el que se indique la acreditación (y para qué Estado). • Habilitar un hipervínculo del logotipo de acreditación con el sitio de acreditación del Estado. El sitio de acreditación del Estado debería incluir detalles sobre el servicio para el que está acreditado el proveedor, además de la fecha de acreditación y la fecha de vencimiento.	✓ ✓ ✓ ✓	 ✓
Aplicar con el ISP acuerdos de nivel de servicios y de mantenimiento que garanticen una disponibilidad adecuada a la importancia del sitio	Disponibilidad	• Definir un acuerdo de nivel de servicios con los ISP que abarquen interrupción del servicio, disponibilidad y anchura de banda. • Definir un contrato de mantenimiento del soporte físico para la infraestructura física, en el que se podrían incluir los acuerdos de nivel de servicios. • Garantizar que los ISP elegidos pueden suministrar suficiente anchura de banda, inclusive volumen suplementario para cualquier crecimiento previsto.	✓ ✓ ✓	
Garantizar que el diseño del sistema proporciona una capacidad y redundancia apropiadas a la importancia del sitio	Disponibilidad	• Reducir al mínimo el número de puntos únicos de falla o las repercusiones de cualquier falla. • Mantener reserva activa/reserva en frío, material de reserva (según sea necesario) para los equipos clave (servidores, encaminadores, etc.) de manera de resolver rápidamente las fallas. • Calcular los requisitos de capacidad del sistema (es decir, aplicando diseños de las mejores prácticas o ensayando la carga del sistema). • Calcular el tamaño de la infraestructura física de acuerdo a la capacidad estimada. • Utilizar agrupaciones de servidores/parque de servidores y equilibradores de carga. • Utilizar unidades de disco de intercambio activas/RAID para reducir al mínimo los efectos de la falla de discos. • Emplear almacenamientos dobles (réplicas de datos). • Emplear una infraestructura de red doble (inclusive con conexión a la Internet a través del ISP) — no son necesarias diferentes compañías si una misma puede proporcionar una infraestructura resistente. • Emplear contratos de suministradores dobles (si no necesariamente de fabricantes) para soporte físico e infraestructura de red — en el caso de caída financiera o medidas reivindicativas. • Emplear servidores con sistema de alimentación ininterrumpida (SAI) para cubrir períodos cortos de falla eléctrica. • Emplear SAI con equipo de reserva con generador diesel para cubrir los períodos más largos de falla eléctrica. • Mantener una infraestructura independiente completa para recuperación de fallas catastróficas y continuidad del servicio.	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	 ✓ ✓ ✓ ✓ ✓

Estrategia para la reducción de riesgos	Categoría de sensibilidad	Mejores prácticas actuales	Se utiliza si la gravedad de las repercusiones es	
			Baja	Alta
Garantizar que el diseño del sistema, arquitectura de la red y los procedimientos de gestión de la vida útil controlan, a un nivel aceptable, la probabilidad de que se pueda desactivar la plataforma por actos malintencionados (intrusos informáticos, virus, gusanos informáticos, denegación de servicio, denegación distribuida de servicio, inundación, etc.) Garantizar que el diseño del sistema, arquitectura de la red, procedimientos de gestión de la vida útil y procedimientos de capacitación controlan, a un nivel aceptable, la probabilidad de que se pueda desactivar la plataforma por actos benévolos	Disponibilidad	• Aplicar una estrategia de fortalecimiento del sistema que garantice que el sistema tiene un nivel adecuado de solidez por medio del retiro o desactivación de todos los componentes que no son necesarios para su función. En esta medida se pueden incluir restricciones de acceso (puertos y protocolos), limitación de la cantidad de usuarios, políticas de contraseña, controles de acceso, derechos de usuario y de grupo y detección de intrusiones.	✓	
		• Aplicar una estrategia de parches de soporte lógico que actualice y mantenga el soporte lógico del sistema a nivel adecuado.		✓
		• Emplear soporte físico anti-DOS — filtros de paquetes/encaminadores “seguros”.	✓	
		• Garantizar que se emplea soporte lógico anti-virus actualizado.		✓
		• Emplear soporte lógico anti-virus de diferentes proveedores para reducir la posibilidad de que un punto vulnerable pueda afectar al proveedor de servicios.	✓	
		• Determinar el acceso de usuarios/patrones de utilización y volumen de tráfico previstos.	✓	
		• Calcular suficiente anchura de banda para atender los patrones de utilización y los volúmenes de tráfico.	✓	
		• Definir los procedimientos de prueba adecuados para garantizar que cuando se introduce un mejoramiento del servicio, es funcional y no tiene repercusiones negativas en el suministro de servicios.	✓	
		• Definir procedimientos de implantación adecuados para garantizar que cuando se introduce un mejoramiento del servicio es funcional y no tiene efectos negativos en el suministro de servicios.		✓
		• Garantizar que ninguna cuenta de usuario puede mantener sesiones paralelas con origen en varias direcciones IP.		✓
		• Implantar una aplicación segura contra fallas (automatizada) que esté disponible en el caso de que el sitio principal estuviera fuera de línea.		✓
		• Utilizar capacitación del personal y procedimientos adecuados para el desarrollo, implantación y mantenimiento del servicio.		✓
		• Vigilar durante 24 horas al día, los siete días de la semana, la infraestructura y aplicaciones con resolución bien documentada o procedimientos de intensificación para cuestiones previstas.		✓

Capítulo 4

CUESTIONES RELATIVAS A LA INFORMACIÓN METEOROLÓGICA

4.1 INTRODUCCIÓN

De conformidad con el Anexo 3 — *Servicio meteorológico para la navegación aérea internacional*, los Estados contratantes acuerdan proporcionar una variedad de servicios que incluye, como mínimo, observaciones y pronósticos que respalden las decisiones operacionales de los centros de control de área, centros de información de vuelo, empresas explotadoras de aeronaves, tripulaciones de vuelo o el piloto al mando. La finalidad de este capítulo es determinar el tipo de información meteorológica que se puede proporcionar a través de la Internet y en qué contexto.

4.2 MENSAJES METEOROLÓGICOS PARA LOS QUE EL TIEMPO ES PRIMORDIAL

4.2.1 La información meteorológica que se enumera en 4.2.2, si se proporciona a través de la Internet, no debería estar relacionada con decisiones operacionales en las que el tiempo sea primordial, tanto en vuelo o inmediatamente antes de la salida. Este tipo de información se denominará información meteorológica para la que el tiempo es primordial, y cuando se utilice en este contexto, se debería distribuir a través del servicio fijo aeronáutico (AFS) ya que sus características garantizarán que tales mensajes se reciban de manera oportuna.

4.2.2 De conformidad con el Anexo 10 — *Telecomunicaciones aeronáuticas*, Volumen II, la información o productos que contienen información meteorológica aeronáutica se clasifican dentro de una de las dos categorías: “mensaje relativo a la seguridad de vuelo” y “mensaje meteorológico”. Los mensajes relativos a la seguridad de vuelo que se refieren a la meteorología aeronáutica, para los que se puede considerar que el tiempo es primordial en el contexto anterior, incluyen:

a) información SIGMET;

b) aeronotificaciones (AIREP) especiales;

c) mensajes AIRMET;

d) avisos de cenizas volcánicas;

e) avisos de ciclones tropicales; y

f) pronósticos de aeródromo (TAF) enmendados.

4.3 MENSAJES METEOROLÓGICOS PARA LOS QUE EL TIEMPO NO ES PRIMORDIAL

4.3.1 Se considera que, para la información meteorológica siguiente el tiempo no es primordial, y se puede proporcionar a través de la Internet:

a) información meteorológica relativa a pronósticos, es decir, TAF, pronósticos de área y de ruta, y la información relativa a observaciones tales como las correspondientes a informes meteorológicos de aeródromo ordinarios (METAR) e informes meteorológicos aeronáuticos especiales de aeródromo (SPECI);

b) información meteorológica que proporcionen los centros mundiales de pronósticos de área (WAFC), es decir, mapas del tiempo significativo y mapas del viento, de la temperatura y de la humedad relativa;

c) formatos gráficos de los avisos de cenizas volcánicas (VAG) que proporcionan los centros de avisos de cenizas volcánicas;

d) pronósticos de área GAMET; y

e) pronósticos de ruta (ROFOR).

Nota.— Los datos mencionados pueden estar en forma binaria universal de representación de datos meteorológicos (BUFR) y datos meteorológicos procesados como valores reticulares expresados en forma binaria (GRIB).

4.3.2 Se considera que para los servicios destinados a explotadores y miembros de la tripulación de vuelo para la planificación previa al vuelo dentro del control operacional centralizado el tiempo no es primordial. Entre la información meteorológica para la planificación previa al vuelo por los explotadores se puede incluir la siguiente:

a) vientos en altitud actuales y previstos, temperaturas en altitud, hasta alturas de la tropopausa, alturas geopotenciales e información sobre vientos máximos y enmiendas correspondientes;

b) tiempo significativo en ruta existente y previsto e información sobre corriente en chorro y enmiendas correspondientes;

c) previsiones para el despegue;

d) METAR y, cuando esté disponible, SPECI para el aeródromo de salida, aeródromos de alternativa de despegue y en ruta, el aeródromo de aterrizaje previsto y aeródromos de alternativa de destino, según se haya determinado en el acuerdo regional de navegación aérea;

e) TAF y enmiendas correspondientes para el aeródromo de salida y de aterrizaje previsto, y para aeródromos de alternativa de despegue, en ruta y de destino, según se haya determinado en el acuerdo regional de navegación aérea; y

f) información SIGMET y aeronotificaciones especiales adecuadas en relación con la totalidad de las rutas correspondientes, según se haya determinado en el acuerdo regional de navegación aérea.

Capítulo 5

CUESTIONES RELATIVAS A LOS SERVICIOS DE INFORMACIÓN AERONÁUTICA (AIS)

5.1 INTRODUCCIÓN

5.1.1 La finalidad de este capítulo es señalar el tipo de información aeronáutica que se puede proporcionar a través de la Internet y en qué contexto.

5.1.2 Se han establecido las Normas y métodos recomendados internacionales (SARPS) del Anexo 15 — *Servicios de información aeronáutica*, y del Anexo 4 — *Cartas aeronáuticas*, y los textos de orientación que figuran en el *Manual para los servicios de información aeronáutica* (Doc 8126) para alcanzar uniformidad y coherencia en el suministro de información aeronáutica.

5.1.3 Aunque los servicios de información aeronáutica que se suministran a través de la Internet se pueden ajustar a las necesidades operacionales de los usuarios (personal de operaciones de vuelo, inclusive tripulaciones de vuelo, planificación de vuelos y simuladores de vuelo, así como la dependencia de servicios de tránsito aéreo responsable del servicio de información de vuelo y de los servicios responsables de la información previa al vuelo), deben conformarse a las normas mencionadas anteriormente.

5.1.4 Se debería establecer un sistema de gestión de la calidad que suministre a los usuarios la garantía y confianza necesarias de que la información aeronáutica distribuida satisface los requisitos estipulados en materia de calidad y rastreo de datos (véase el Anexo 15, Capítulo 3, 3.2.5).

5.2 INFORMACIÓN AERONÁUTICA EN LA QUE EL TIEMPO ES PRIMORDIAL

5.2.1 Se considera que para la siguiente información aeronáutica el tiempo es primordial y, cuando se suministre a través de la Internet, no habría que basarse en ella en decisiones operacionales en las que el tiempo es primordial, ni durante los vuelos o inmediatamente antes de la salida:

a) información dinámica de carácter provisional, como los NOTAM nacionales y extranjeros actuales (inclusive SNOWTAM, ASHTAM y listas de verificación); y

b) otro tipo de información de carácter urgente que se ponga a disposición de las tripulaciones de vuelo en forma de boletines de información previa al vuelo (PIB) en lenguaje claro.

5.2.2 En el Anexo 15, Capítulo 5, 5.3.2.1, se especifica que, siempre que sea posible, se empleará el AFS para la distribución de los NOTAM.

5.2.3 Es necesario que al proporcionar boletines de información previa al vuelo de valor añadido o productos con formatos y gráficos personalizados, cuando corresponda, se proporcionen como mínimo los servicios que estarían disponibles en forma impresa.

5.3 INFORMACIÓN AERONÁUTICA EN LA QUE EL TIEMPO NO ES PRIMORDIAL

Se considera que en la información AIS estática o básica siguiente el tiempo no es primordial y se puede suministrar a través de la Internet:

a) ***Información estática***. Información común en documentos permanentes o a largo plazo, como:

1) publicaciones de información aeronáutica (AIP) [en las que figura información de aeródromos, descripciones detalladas de regiones de información de vuelo (FIR), ayudas para la navegación aérea, mapas, cartas, datos sobre obstáculos, rutas aéreas, etc.];

2) enmiendas AIP, tanto reglamentación y control de información aeronáutica (AIRAC) como enmiendas ordinarias;

3) Suplementos AIP, tanto AIRAC como suplementos ordinarios;

4) circulares de información aeronáutica (AIC);

5) lista mensual impresa en lenguaje claro de NOTAM válidos, en la que se incluyan también indicaciones de las últimas enmiendas AIP, AIC publicadas y una lista de verificación de suplementos AIP; y

6) NOTAM en que figure una lista de verificación de NOTAM válidos, impresa mensualmente, en la que también se haga referencia a las últimas enmiendas AIP, suplementos AIP y como mínimo las AIC distribuidas internacionalmente.

b) ***Información básica***. Los datos necesarios para permitir el procesamiento de otro tipo de información, que puede consistir en datos permanentes, a largo plazo o estáticos no suministrados a los usuarios (es decir, listas de referencia, rutas por clientes u ordinarias, archivos de distribución, criterios de selección, criterios de asociación).

5.4 SUMINISTRO DE INFORMACIÓN ESTÁTICA Y BÁSICA

5.4.1 La información estática y básica puede ser permanente o de larga duración. Es necesario señalar la fecha de vigencia de la información. Cada publicación deberá estar fechada. Si las páginas tienen diferentes vigencias, cada página deberá estar fechada por separado. En el caso en que los elementos de los datos estén publicados de manera independiente, es necesario que tengan una fecha de vigencia determinada.

5.4.2 Las fechas de vigencia comunes, a intervalos de 28 días en virtud del sistema reglamentado (AIRAC), se deberán utilizar para la información enumerada en el Anexo 15, Apéndice 4, Parte 1 y se recomiendan además para la información que se enumera en la Parte 2 (en el Capítulo 6 del Anexo 15 se suministran detalles). Para facilitar la transición de una fecha de vigencia a la próxima fecha de publicación (fecha de ciclo AIRAC), se debe suministrar la información aeronáutica anterior, actual y para el próximo ciclo para un período determinado. Cuando se pone a disposición un servicio de esta naturaleza, es cada vez más importante que se determine claramente la fecha de vigencia para toda la información aeronáutica.

5.4.3 La Internet se puede utilizar para suministrar información en el marco del sistema AIRAC. Sin embargo, se debe disponer lo necesario para el suministro de información en forma impresa (véase la Sección 6.2 del Anexo 15). El sistema AIRAC está destinado a suministrar información planificada anteriormente a receptores determinados: terceros proveedores de AIS, organismos aeronáuticos, productores de cartas y bases de datos, etc. Se recomienda la confidencialidad (véase el Capítulo 3 de este manual). Es necesario que las organizaciones que prevén suministrar este tipo de información se aseguren de que los usuarios tienen buen conocimiento del sistema AIRAC y están bien al tanto de la aplicación de fechas relacionadas con la información.

5.5 SUMINISTRO DE CARTAS

5.5.1 Las disposiciones que figuran en los Anexos 4 y 15 se aplican al contenido y presentación visual de los tipos de cartas del Anexo 4 de la OACI y otras cartas AIP, inclusive las que ponen a disposición los servicios de información aeronáutica del Estado a través de la Internet. Las cartas se deberán presentar a escalas que sean compatibles con los requisitos del Anexo 4. Si se permite trazar a escala una carta, los usuarios deberán estar informados de la gradación de la escala que permitirá mantener la calidad de la carta. Se ha previsto que, próximamente, la mayor parte de las cartas que se pongan a disposición a través de la Internet tendrán una presentación visual idéntica a las actuales cartas impresas. Sin embargo, algunos sistemas de información geográfica (GIS) y cartográfica están en condiciones de suministrar cartas en formatos con mayor funcionalidad, incluyendo la posibilidad de que los usuarios controlen el tipo de información presentada. Es importante que, cuando las cartas electrónicas se presentan en tales formatos, toda la información pertinente se presente inicialmente al usuario y que no se pueda eliminar la selección de la información crítica para la seguridad operacional.

5.5.2 Los formatos gráficos óptimos para poner los mapas y cartas en la Internet pueden ser diferentes de los que se utilizan en la producción de documentos y se pueden elegir teniendo en cuenta las siguientes consideraciones generales:

a) la disponibilidad de opciones para la salida gráfica de soportes lógicos o escáneres de producción cartográfica;

b) la disponibilidad, para los clientes, de cartas publicadas (compatibilidad con sistemas operativos, navegadores web, reproducción de colores e impresoras clientes);

c) funcionalidad de la carta y calidad de la imagen;

d) volumen de los datos de la carta (y por lo tanto el tiempo de transferencia); y

e) si el formato es de estándar abierto o comercial, con costos conexos.

Capítulo 6

CUESTIONES RELATIVAS A LOS PLANES DE VUELO

6.1 INTRODUCCIÓN

6.1.1 La finalidad de este capítulo es proporcionar orientación sobre la presentación y gestión de los planes de vuelo [desde y hacia el servicio fijo aeronáutico (AFS)] a través de la Internet.

6.1.2 La Internet se puede utilizar como medio para suministrar aplicaciones para presentar y recolectar planes de vuelo directamente de los usuarios. Además, la Internet permite el intercambio de información sobre la aceptación de los planes de vuelo y la consiguiente consulta y modificación o cancelación de los planes de vuelo presentados. Las aplicaciones de planes de vuelo de Internet a menudo se ofrecen en combinación con aplicaciones AIS y MET que suministran la totalidad de la información aeronáutica requerida.

6.2 PRESENTACIÓN DE LOS PLANES DE VUELO

6.2.1 Se deben observar el formato de plan de vuelo estándar y los criterios de validación que figuran en los *Procedimientos para los servicios de navegación aérea — Gestión del tránsito aéreo* (PANS-ATM, Doc 4444).

6.2.2 La utilización de la Internet para la presentación de los planes de vuelo podría reducir la carga de trabajo manual de las oficinas de notificación de los servicios de tránsito aéreo al ofrecer aplicaciones de usuarios para la recolección de planes de vuelo correctos en su sintaxis y pasarlos de manera segura para su ulterior tramitación en el ambiente operacional de los planes de vuelo.

6.2.3 Se debe tener en cuenta que un sistema puede ser vulnerable a ataques por denegación de servicio (DoS) a través de la interfaz de Internet. Sería posible denegar el acceso al servicio a otros usuarios legítimos mediante la presentación ilimitada e incontrolada de planes de vuelo. Además, en un sistema completamente automatizado, sería también posible afectar a los sistemas operacionales propiamente dichos. Es necesaria la aplicación de procedimientos automáticos o de control manual para reducir el riesgo de ataques DoS.

6.2.4 La presentación de planes de vuelo a través de la Internet se puede ampliar fácilmente a vuelos que no tienen que presentar un plan de vuelo. Por ejemplo, esto podría ayudar a vigilar los vuelos según las reglas de vuelo visual, para fines de búsqueda y salvamento.

6.3 GESTIÓN DE LOS PLANES DE VUELO

6.3.1 La Internet puede suministrar al usuario acceso directo a información tal como acuse de recibo, cambios o rechazo de los planes de vuelo presentados, de manera automatizada y controlada, en tiempo real, con sujeción a la disponibilidad de los medios de comunicación y las interfaces requeridas.

6.3.2 Se debería ofrecer al usuario intercambio de información sobre la aceptación del plan de vuelo, permitiendo consultas consiguientes y modificación o cancelación de la presentación de un plan de vuelo. El riesgo principal para los sistemas operacionales es que las aplicaciones de Internet no cumplan con las interfaces adecuadas para el AFS.

Capítulo 7

OTRAS APLICACIONES

7.1 APLICACIÓN DE MENSAJES DEL TIPO AFTN

7.1.1 Se reconoce que la Internet se está utilizando como un medio alternativo de intercambiar mensajes del tipo AFTN entre Estados en casos excepcionales (es decir, en el caso de que los circuitos especializados no estén disponibles, no sean fiables o no sean económicos debido al bajo nivel de tráfico).

7.1.2 En cualquier implantación de comunicaciones del tipo AFTN basadas en Internet, se deberían observar los procedimientos que figuran en el Anexo 10, Volumen II, en relación con el formato, procesamiento y retención de los mensajes.

7.1.3 Se debería otorgar la debida atención a los procedimientos de evaluación y gestión de riesgos que figuran en el Capítulo 3 de este manual.

— FIN —

PUBLICACIONES TÉCNICAS DE LA OACI

Este resumen explica el carácter, a la vez que describe, en términos generales, el contenido de las distintas series de publicaciones técnicas editadas por la Organización de Aviación Civil Internacional. No incluye las publicaciones especializadas que no encajan específicamente en una de las series, como por ejemplo el Catálogo de cartas aeronáuticas, *o las* Tablas meteorológicas para la navegación aérea internacional.

Normas y métodos recomendados internacionales. El Consejo los adopta de conformidad con los Artículos 54, 37 y 90 del Convenio sobre Aviación Civil Internacional, y por conveniencia se han designado como Anexos al citado Convenio. Para conseguir la seguridad o regularidad de la navegación aérea internacional, se considera que los Estados contratantes deben aplicar uniformemente las especificaciones de las normas internacionales. Para conseguir la seguridad, regularidad o eficiencia, también se considera conveniente que los propios Estados se ajusten a los métodos recomendados internacionales. Si se desea lograr la seguridad y regularidad de la navegación aérea internacional es esencial tener conocimiento de cualesquier diferencias que puedan existir entre los reglamentos y métodos nacionales de cada uno de los Estados y las normas internacionales. Si, por algún motivo, un Estado no puede ajustarse, en todo o en parte, a determinada norma internacional, tiene de hecho la obligación, según el Artículo 38 del Convenio, de notificar al Consejo toda diferencia o discrepancia. Las diferencias que puedan existir con un método recomendado internacional también pueden ser significativas para la seguridad de la navegación aérea, y si bien el Convenio no impone obligación alguna al respecto, el Consejo ha invitado a los Estados contratantes a que notifiquen toda diferencia además de aquéllas que atañan directamente, como se deja apuntado, a las normas internacionales.

Procedimientos para los servicios de navegación aérea (PANS). El Consejo los aprueba para su aplicación mundial. Comprenden, en su mayor parte, procedimientos de operación cuyo grado de desarrollo no se estima suficiente para su adopción como normas o métodos recomendados internacionales, así como también materias de un carácter más permanente que se consideran demasiado detalladas para su inclusión en un Anexo, o que son susceptibles de frecuentes enmiendas, por lo que los procedimientos previstos en el Convenio resultarían demasiado complejos.

Procedimientos suplementarios regionales (SUPPS). Tienen carácter similar al de los procedimientos para los servicios de navegación aérea ya que han de ser aprobados por el Consejo, pero únicamente para su aplicación en las respectivas regiones. Se publican englobados en un mismo volumen, puesto que algunos de estos procedimientos afectan a regiones con áreas comunes, o se siguen en dos o más regiones.

Las publicaciones que se indican a continuación se preparan bajo la responsabilidad del Secretario General, de acuerdo con los principios y criterios previamente aprobados por el Consejo.

Manuales técnicos. Proporcionan orientación e información más detallada sobre las normas, métodos recomendados y procedimientos internacionales para los servicios de navegación aérea, para facilitar su aplicación.

Planes de navegación aérea. Detallan las instalaciones y servicios que se requieren para los vuelos internacionales en las distintas regiones de navegación aérea establecidas por la OACI. Se preparan por decisión del Secretario General, a base de las recomendaciones formuladas por las conferencias regionales de navegación aérea y de las decisiones tomadas por el Consejo acerca de dichas recomendaciones. Los planes se enmiendan periódicamente para que reflejen todo cambio en cuanto a los requisitos, así como al estado de ejecución de las instalaciones y servicios recomendados.

Circulares de la OACI. Facilitan información especializada de interés para los Estados contratantes. Comprenden estudios de carácter técnico.

10/05, S/P1/160

Núm. de pedido 9855
Impreso en la OACI

ISBN 92-9194-606-0