CA/FS No. 041

ACEPTACIÓN DE REGISTROS ELECTRÓNICOS DE MANTENIMIENTO DE AERONAVES (EAMR) Y REGISTROS DE MANTENIMIENTO DE LA AERONAVEGABILIDAD

1) PROPÓSITO:

Esta Circular de Asesoramiento (CA) provee los procedimientos, lineamientos y la información necesaria, para la aceptación de registros electrónicos de mantenimiento de aeronaves (EAMR) y registros de mantenimiento de la aeronavegabilidad.

2) DIRIGIDO A :

Operadores Aereos (COA) y/o Certificadores Operativos (CO), Organizaciones de Mantenimiento aprobada (OMA), Organizaciones de Mantenimiento Reconocidas bajo RAC 145.

3) EXCEPCIONES:

(N/A)

4) AMBITO REGULATORIO:

Anexo 8 de OACI capítulo 6, 6.7, Documento 9760 Adjunto B del Capítulo 7, RAC 145.55.

5) DEFINICION REGISTROS ELECTRONICOS:

Se debe entender el término "registro electrónico" a los registros electrónicos de mantenimiento y los registros de mantenimiento de la aeronavegabilidad de aeronaves, motores, hélices y Componentes.

6) GENERALIDADES:

La información relacionada con el mantenimiento de aeronaves y el mantenimiento de la aeronavegabilidad se suele registrar, certificar y almacenar en papel. Las capacidades de la práctica aceptada del uso de papel no bastan para respaldar registros precisos y completos en tiempo real ante el aumento del volumen y la complejidad de la información sobre la operación y el mantenimiento de aeronaves modernas. La DGAC considera la aprobación y vigilancia de los procesos y procedimientos de mantenimiento de registros electrónicos que deben implementar los explotadores aéreos y los organismos de mantenimiento.

Un sistema de mantenimiento de registros electrónicos debe ser un sistema de procesamiento de registros mediante el cual los registros se ingresan, se aprueban electrónicamente, se almacenan y se recuperan por medios electrónicos en un sistema informático en lugar de en el "formato impreso" tradicional.

Se debe describir todo sistema de mantenimiento de registros electrónicos y el registro que este genera, procesa y almacena en el manual para controlar el mantenimiento del Operador (MCM) y en el Manual de la Organización de Mantenimiento (MOM). Ese sistema debe ser aceptable para la DGAC y cumplir los requisitos establecidos para la actividad operacional y de mantenimiento del Operador. Esto debe incluir el acceso irrestricto de la autoridad con fines de auditoría y la capacidad del organismo de suministrar copias impresas de los registros si así lo requiere la DGAC.

El registro electrónico generado, procesado y almacenado conforme a los requisitos de la DGAC se debe considerar un documento original. La DGAC debería considerar aceptable el uso de un sistema completo de mantenimiento de registros electrónicos. Los registros electrónicos con firma electrónica se deben considerar equivalentes a los registros de mantenimiento de aeronaves y de mantenimiento de la aeronavegabilidad autenticados con firmas no electrónicas.
Toda impresión de un registro electrónico requerida por la DGAC debe tener una marca de agua en el fondo de la página que diga "IMPRESO DESDE UN ARCHIVO ELECTRÓNICO".

El intercambio de registros electrónicos entre organizaciones de aviación, bajo la responsabilidad de vigilancia de la misma DGAC, debería tener lugar de forma voluntaria cuando tanto el expedidor como el receptor convengan en la transferencia electrónica de los registros.

Los registros impresos de mantenimiento de aeronaves deben seguir siendo aceptables para la DGAC si el Operador o el organismo de mantenimiento adoptan el sistema tradicional de documentos impresos.
La DGAC no debe exigir la implementación de un sistema doble si el organismo adoptó un sistema de registro electrónico. Un sistema combinado de mantenimiento de registros electrónicos e impresos debe ser aceptable para la DGAC si el explotador aéreo, el organismo de mantenimiento de aeronaves adoptan el sistema tradicional de registros impresos como sistema de respaldo para situaciones en las que no se puede crear un registro electrónico completo.

La adopción del sistema de registros electrónicos debe estar supeditada a que se pueda impartir a todos los usuarios del sistema la instrucción adecuada que incluya sensibilización en materia de seguridad y políticas y procedimientos relativos al sistema adoptado. Así, la garantía de su implementación resulta tan importante para un sistema de registros electrónicos como la propia arquitectura. La DGAC debe validar, antes de la aceptación del sistema de registros electrónicos, no solo las capacidades técnicas del sistema propuesto, sino también la preparación del organismo para adoptar el sistema.

7) IDENTIFICACION, AUTENTICACION Y AUTORIZACION:

La base de todo registro electrónico y su sistema conexo de gestión de identidad de firma electrónica es la confianza. Ya sea que se trate de identificar una aeronave, un miembro de la tripulación, un mecánico, un componente o una estación terrestre, el organismo deberá poder confiar en que, cuando la entidad presenta una credencial digital, esa Credencial fue expedida a dicha entidad y está vinculada con ella. Para contribuir a establecer la confianza, se deben especificar requisitos y procedimientos que permitan y garanticen la verificación de la identidad de las diversas partes que participan en la expedición de una credencial. La credencial debe ser la base para establecer la identidad de un usuario de un sistema de registros electrónicos.

El sistema de registros electrónicos debe autenticar la identidad del usuario. La autenticación debe consistir en medios por los cuales el sistema valida la identidad de un usuario autorizado. Estos medios pueden incluir, entre otros, una contraseña, un número de identificación personal (PIN), una clave criptográfica o una credencial que se pasa por un lector, todo ello, en correlación con la solución y los procesos implementados.

El nivel de garantía de identidad y autenticación debe ser acorde a la clase de actividad para la que el sistema de registros electrónicos autoriza el acceso del usuario.

La garantía de identidad del usuario debe comprender procedimientos tanto iniciales como continuos (es decir, periódicos) que el usuario debe cumplir.

El organismo al que pertenece el usuario en el momento de interactuar con el registro electrónico debe ser responsable de la correlación entre la gestión de la identidad del usuario y el alcance de la autorización de ese usuario.

9. FIRMA ELECTRONICA:

El uso de la expresión "firma electrónica" tiene por objeto abarcar categorías amplias y diversas de soluciones que, si bien se pueden identificar de otra manera en el campo especializado de la seguridad digital de acuerdo con sus características y capacidades tecnológicas. La inexactitud generada por la falta de diferenciación entre categorías tales como firma electrónica, firma digital, firma electrónica avanzada, firma electrónica segura o firma electrónica digital se considera irrelevante en lo que respecta a estas directrices.

La firma manuscrita es de aceptación universal porque tiene ciertas cualidades y atributos que se deben conservar en cualquier firma electrónica. La firma electrónica aceptable tiene idéntico propósito que el de una firma manuscrita; por tanto, una firma electrónica debe poseer aquellas cualidades y atributos que garanticen la autenticidad de una firma manuscrita.

Se pueden utilizar sistemas de mantenimiento de registros electrónicos para generar registros de aeronaves (p. ej., tarjetas de tareas de mantenimiento, registros de mantenimiento de aeronaves, conformidades de despacho, conformidades de vuelo, conformidades de

aeronavegabilidad e informes de pruebas de vuelo) para los cuales es necesario poder autenticar adecuadamente al usuario que usa la firma electrónica.

La firma electrónica es el equivalente en línea de una firma manuscrita. Es un sonido, símbolo, marca visible o proceso electrónico adjunto o asociado lógicamente con un registro y ejecutado o adoptado por una persona con la intención de firmar el registro. Identifica y autentica electrónicamente a una persona que ingresa, verifica o audita registros informáticos. La firma electrónica debe proporcionar una autenticación segura del firmante y debe estar vinculada a los datos para los que se creó la firma de tal manera que todo cambio posterior de los datos sea detectable.

Existen varios atributos que debe poseer una firma electrónica:

Singularidad, que es la característica por la cual la firma electrónica debe identificar a una persona específica y solo a esa persona y debe ser difícil de duplicar. Un método aceptable para demostrar la singularidad de una firma es utilizar un procedimiento de identificación y autenticación que valide la identidad del firmante. Entre los medios aceptables de identificación y autenticación, cabe mencionar el uso de códigos de identificación y autenticación separados y no relacionados. Pueden estar codificados en credenciales, tarjetas, claves criptográficas u otros objetos. Los sistemas que utilizan PIN o contraseñas también podrían ser un método aceptable para garantizar la singularidad. Una entrada de computadora utilizada como firma debe tener acceso restringido limitado por un código de autenticación que se cambia periódicamente. Además, un sistema podría utilizar características físicas, como una huella digital, una huella de la mano o un patrón de voz, como método de identificación y autorización.

Relevancia, que es la característica por la cual una persona que usa una firma electrónica debe llevar a cabo una acción deliberada y reconocible para colocar su firma. Las acciones deliberadas y aceptables para crear una firma electrónica digital incluyen: pasar la credencial, firmar un documento electrónico con un lápiz óptico, pulsar teclas específicas o usar una firma digital.

Alcance, que es la característica por la cual el alcance de la información que se declara con una firma electrónica debe ser claro para el firmante y para los posteriores lectores del registro, entrada de registro o documento. El registro electrónico debe reflejar con precisión la información declarada por el firmante y este debe ser plenamente consciente de lo que está firmando.

Seguridad, que es la característica por la cual un sistema electrónico que produce firmas debe restringir la posibilidad de que las personas coloquen la firma de otra persona en un registro, entrada de registro, documento o alteren el contenido sin dejar rastro. A tal efecto, una política y una estructura de gestión acordes deberían respaldar los soportes físico y lógico de la computadora destinados a suministrar la información. El sistema debe contener restricciones y procedimientos para prohibir el uso de la firma electrónica de una persona cuando esta deja de trabajar. Esto debe hacerse inmediatamente después de la notificación del cambio en la situación laboral de esa persona.

No repudio, que es la característica mediante la cual una firma electrónica debe evitar que un firmante niegue haber estampado una firma en un registro, entrada de registro o documento específico.

Trazabilidad, que es la característica por la cual una firma electrónica debe proporcionar una trazabilidad positiva a la persona que firmó un registro, entrada de registro o cualquier otro documento.

La solución de firma electrónica adoptada debe cumplir los requisitos validados y las normas de la industria con respecto a: la solidez de la credencial de identificación del usuario/sistema empleada en la creación de firmas, el algoritmo de prueba de posesión para las credenciales de identificación, el algoritmo criptográfico para la protección de datos y alternativas que pueden proporcionar una protección similar si los anteriores no se consideran prácticos.

Los registros electrónicos están esencialmente vinculados en la mayoría de los casos a la información de fecha y hora en que fueron creados, modificados y firmados. Dicha información se debe tratar de manera adecuada mediante la función de marca horaria del sistema de mantenimiento de registros electrónicos.

10. SEGURIDAD E INTEGRIDAD:

Una política y una estructura de gestión acordes deben respaldar los soportes físico y lógico de la Computadora que suministran la información. Se deben establecer procedimientos apropiados de seguridad física y copia de seguridad de los registros electrónicos para los registros actuales, operacionales, almacenados y archivados. El sistema de registros electrónicos debe proteger la información confidencial.

El sistema de registros electrónicos debe garantizar que la información no se vea alterada por cambios no autorizados en el registro.

Se deben establecer procedimientos que permitan al organismo corregir documentos que fueron firmados electrónicamente por error. Se debe reemplazar la entrada original siempre que se efectúe una corrección relacionada con esa entrada. (La entrada original debe quedar anulada pero no eliminada. Se debe hacer referencia a una nueva entrada, que es preciso firmar y fechar electrónicamente). Se debe indicar con claridad que la entrada original ha sido reemplazada por otra entrada.

Deben establecerse procedimientos para describir la manera en que el explotador garantizará que los registros electrónicos se transmitan de conformidad con los requisitos reglamentarios apropiados a las partes interesadas que necesitan acceder a los registros.

Se deben establecer procedimientos para examinar el sistema informático de códigos de identificación personal para garantizar que el sistema no permita duplicar contraseñas.

Se deben establecer procedimientos para auditar el sistema informático de forma periódica a fin de garantizar la integridad del sistema. Se debe completar y conservar en archivo un registro de la

auditoría como parte de los requisitos de conservación de registros del explotador. Esa auditoría puede estar respaldada por la autocomprobación automática del sistema.

Se deben establecer procedimientos para auditorías no periódicas del sistema informático si se duda de la integridad del sistema.

Se deben establecer procedimientos de auditoría para garantizar la integridad de cada estación de trabajo computarizada. Si las estaciones de trabajo están conectadas a un servidor y no contienen atributos inherentes que habiliten o deshabiliten el acceso, no es necesario auditar cada una de ellas. Los procedimientos deben ser aplicables tanto a equipos fijos (por ejemplo, computadoras de escritorio) como móviles (por ejemplo, computadoras portátiles,
tabletas, terminales portátiles de acceso para mantenimiento, etc.).

Se debe establecer un proceso de evaluación de la seguridad informática para el sistema de registros electrónicos a fin de determinar la eficacia con la que cada entidad que se evalúa (por ejemplo, host, red, procedimiento, persona) cumple los objetivos de seguridad específicos. La implementación efectiva de ese proceso establecido debe contemplar procedimientos de prueba de descifrado de contraseñas y de penetración de la seguridad.

11. ARCHIVOS Y TRANSFERIBILIDAD :

Además de la seguridad física de los archivos, se deben establecer procedimientos específicos para el archivo de documentos firmados electrónicamente. Todo software informático de firma electrónica debería contar con un medio para archivar de forma segura documentos firmados electrónicamente. Esto contemplará y respaldará adecuadamente la conservación, el acceso y la autenticación futura de los registros electrónicos.

Se deben establecer procedimientos para velar por que todos los registros de mantenimiento de las aeronaves y mantenimiento de la aeronavegabilidad, estén disponibles durante la transferencia de aeronaves para respaldar el certificado de aeronavegabilidad para
Exportación. El sistema de mantenimiento de registros electrónicos debe incluir el protocolo necesario para permitir la transferencia segura de los registros a otro sistema de mantenimiento de registros electrónicos.

Autorizado:

DIRECCION GENERAL DE AERONAUTICA CIVIL
DGAC
Despacho Superior
GUATEMALA, C. A.

P.A. Francis Arturo Argueta Aguirre
Director General
Dirección General de Aeronáutica Civil