

**PERÚ****Ministerio  
de Transportes  
y Comunicaciones****Viceministerio  
de Transportes****Dirección General  
de Aeronáutica Civil**

## CIRCULAR DE ASESORAMIENTO

CA : CA-314-2.1.6-2018  
FECHA : 04/07/2018  
EDICIÓN : ORIGINAL  
EMITIDA POR: DSA-DGAC

**ASUNTO: VERIFICACION DE LA INTEGRIDAD DE LOS ARCHIVOS DE DATOS**

### 1. PROPÓSITO

La presente Circular de Asesoramiento (CA) proporciona una herramienta y orientación para la verificación de la integridad de los archivos de datos de aeródromos en el momento del intercambio.

### 2. ALCANCE

Esta Circular de Asesoramiento está orientada a proporcionar una guía a los originadores de datos y/o explotadores de aeródromos.

### 3. BASE LEGAL

- RAP 314, Volumen I: Diseño y Operaciones de Aeródromos.
- RAP 314, Volumen II: Helipuertos
- RAP 315: Servicio de Información Aeronáutica

### 4. DOCUMENTOS RELACIONADOS

- Manual del Sistema Geodésico Mundial 1984 – WGS 84. Doc. 9674-AN/946

### 5. DEFINICIONES Y ACRONIMOS

- a) **Algoritmo:** es un conjunto de instrucciones o reglas bien definidas, ordenadas y finitas que permiten llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad.
- b) **Aeropuerto:** Todo aeródromo especialmente equipado y usado regularmente para pasajeros y carga en el tráfico aéreo. Todo aeródromo que a juicio de la Autoridad Aeronáutica, posee instalaciones suficientes para ser consideradas de importancia en la aviación civil o el que defina la Ley.
- c) **Explotador de Aeródromo:** Es la persona Natural o Jurídica consignada en la autorización de funcionamiento, obligada a mantener o conservar el aeródromo y a comunicar a la DGAC las limitaciones temporales o permanentes que afecten su uso.
- d) **SHA256:** Es un conjunto de funciones denominadas hash, diseñadas por la Agencia de Seguridad Nacional (NSA), una función hash es un algoritmo que transforma un conjunto arbitrario de elementos de datos, en único valor de longitud fija. El valor calculado puede ser utilizado para la verificación de la integridad de un dato original.
- e) **CRC:** Ciclo de comprobación de datos electrónicos por redundancia cíclica.
- f) **Integridad:** Grado de garantía de que no se han perdido ni alterado ninguna de las referencias Aeronáuticas ni sus valores después de la referencia o enmienda autorizada.

- g) **Verificación de la integridad de datos aeronáuticos:** Tiene por objetivo garantizar la integridad de los datos aeronáuticos electrónicos que son suministrados a la Autoridad Aeronáutica, y proporciona un medio para identificar posibles problemas en el envío y almacenamiento de datos aeronáuticos electrónicos.

## 6. ABREVIATURAS

- a. **RAP** Regulación Aeronáutica del Perú.
- b. **CA** Circular de asesoramiento.
- c. **DGAC** Dirección General de Aeronáutica Civil.
- d. **AIP** Publicación de información aeronáutica.
- e. **MTC** Ministerio de Transporte y Comunicaciones

## 7. ORIENTACION Y PROCEDIMIENTOS

### 7.1 COMPROBACION Y PROTECCION DE INTEGRIDAD Y EXACTITUD DE DATOS AERONAUTICOS ELECTRONICOS

7.2 La DGAC se asegurará de que el Explotador de Aeródromo cumpla con los siguientes requisitos:

7.2.1 Integridad de los datos aeronáuticos: se basarán en el posible riesgo derivado de la alteración de los datos y del uso al que se destinen. En consecuencia, el Explotador de Aeródromo aplicará la siguiente clasificación de integridad de datos:

- 1) Datos críticos: existe gran probabilidad de que utilizando datos críticos alterados, la continuación segura del vuelo y el aterrizaje de la aeronave se pondrán en grave riesgo con posibilidades de catástrofe;
- 2) Datos esenciales: existe baja probabilidad de que utilizando datos esenciales alterados, la continuación segura del vuelo y el aterrizaje de la aeronave se pondrán en grave riesgo con posibilidades de catástrofe,
- 3) Datos ordinarios: existe muy baja probabilidad de que utilizando datos ordinarios alterados, la continuación segura del vuelo y el aterrizaje de la aeronave se pondrán en grave riesgo con posibilidades de catástrofe.

7.2.2 La protección de los datos aeronáuticos electrónicos almacenados o en tránsito serán supervisados por la DGAC mediante un algoritmo matemático de verificación de integridad de datos. Para lograr la protección del nivel de integridad de los datos aeronáuticos críticos, esenciales y ordinarios clasificados en 7.2.1, el Explotador del Aeródromos aplicará respectivamente un algoritmo matemático.

### 7.3 Algoritmo de Integridad de los datos (SHA256)

7.3.1 La función hash criptográfica SHA256 se emplea para comprobar la integridad de un archivo de datos, es decir, para poder saber si ha sido modificado o se mantiene intacto desde su origen.

7.3.2 Para cada archivo con datos transmitido desde los originadores al siguiente usuario, con el fin de verificar la integridad de los datos en el momento del intercambio, se incluirá un archivo de verificación SHA256 asociado con su mismo nombre, y extensión “.sha”.

7.3.3 El archivo de verificación SHA256 es un archivo de texto que contiene, entre otros datos, el valor de hash SHA256, que permite comprobar la integridad de un archivo. La DGAC pone a disposición de los originadores, a través de la página web del MTC, un programa de cálculo de códigos SHA256 para verificar la integridad de los archivos de datos.

- 7.3.4 Cuando el siguiente usuario reciba el archivo, comprobará el valor de hash SHA256. Si coincide con el transmitido se iniciará su tratamiento, en caso contrario, se solicitará de nuevo el archivo al originador.
- 7.4 Instrucciones para crear el archivo de verificación SHA para el envío de archivos de datos
- 7.4.1.1 Acceda a la aplicación desde la página web del Ministerio de Transportes y comunicaciones en la pestaña de Aeronáutica Civil.
- 7.4.2 Seleccione el o los archivos de datos
- 7.4.3 El programa generara un enlace para descargar el archivo SHA asociado a cada archivo de datos
- 7.4.3.1 Descargar todos los archivos SHA generados y copiarlos junto a los archivos de datos
- 7.4.4 Verificar que los archivos de datos son los correctos: Si se guardan o modifican los archivos de datos se debe eliminar los archivos SHA y volver al numeral 7.4.1 para generarlos de nuevo.
- 7.4.5 Enviar los archivos de datos y SHA al siguiente usuario.
- 7.5 Instrucciones para verificar archivos de datos recibidos junto con su SHA
- 7.5.1 Seleccione el o los archivos de datos juntos con sus archivos de extensión sha
- 7.5.2 El programa comprobara la integridad mostrando el resultado en pantalla

The screenshot shows the DGAC Peru website header with the logo and text "Dirección General de Aeronáutica Civil" and "coordinacion tecnica de aerodromos". Below the header is a language selector set to "Español". The main content area is titled "Verificación de la Integridad Datos de Aerodromos" and contains a section "Genera/Comprueba SHA256" with a large dashed box labeled "Seleccione Archivo". Below this are two instruction sections: "Instrucciones para crear archivo de verificación SHA para el envío de archivos de datos" and "Instrucciones para verificar archivos de datos recibidos junto con su SHA". The footer contains "DGAC Peru 2018" and "Version 1.0.0".

**DGAC** Dirección General de Aeronáutica Civil  
PERU

coordinacion tecnica de aerodromos

Español

Verificación de la Integridad Datos de Aerodromos

Genera/Comprueba SHA256

Seleccione Archivo

**Instrucciones para crear archivo de verificación SHA para el envío de archivos de datos**

1. Seleccione el o los archivos de datos (para archivos de mas de 500MB se recomienda usar Firefox)
2. El programa generara un enlace para dercargar el archivo SHA asociado a cada archivo de datos
3. Descargar todos los archivos SHA generados y copiarlos junto a los archivos de datos
4. Verificar que los archivos de datos son los correctos: Si se guardan o modifican los archivos de datos se debe eliminar los archivos SHA y volver al paso 1 para generarlos de nuevo.
5. Enviar los archivos de datos y SHA al siguiente usuario

**Instrucciones para verificar archivos de datos recibidos junto con su SHA**

1. Seleccione el o los archivos de datos juntos con sus archivos sha
2. El programa comprobara la integridad mostrando el resultado en pantalla

DGAC Peru 2018 Version 1.0.0