

1. Introducción

El Instituto Dominicano de Aviación Civil, en adelante IDAC, ente público especializado y técnico, con personalidad jurídica, patrimonio propio, poder de reglamentación, de decisión y autoridad para implementar su organización interna, en el marco de cumplimiento de su Política de Seguridad de Información ha decidido establecer las categorías de clasificación de su información.

Esta política tiene por objeto:

- Establecer las categorías de clasificación de los datos e información institucional.
- Disponer las pautas de clasificación, rotulación y manejo de los datos e información.
- Dictar los lineamientos para almacenamiento, reproducción, eliminación, transporte y destrucción de información confidencial.

2. Alcance

Esta política es aplicable a todos los empleados y funcionarios del IDAC que por sus funciones tengan acceso a cualquier dato e información del IDAC, a través de cualquier medio, sea este electrónico, analógico, visual, auditivo o gestual, en cualquiera de sus instalaciones u operaciones locales o remotas.

3. Clasificación de la información

El IDAC ha clasificado su información en las siguientes categorías:

- a) **Pública:** Esta información debe estar al alcance, tanto de los empleados del organismo gubernamental como del público externo. Es posible su divulgación tanto externa como interna sin restricciones.
- b) **Interna:** Esta información se utiliza para las operaciones del IDAC y debe estar solo al alcance de sus empleados y funcionarios. Su divulgación no autorizada causa incomodidad menor o inconveniencia operativa menor.
- c) **Sensitiva:** Esta información debe estar solo al alcance de personas autorizadas. Su divulgación no autorizada tiene un impacto significativo a corto plazo en las operaciones o los objetivos estratégicos y/o tácticos.
- d) **Confidencial:** Esta información debe estar disponible para un personal autorizado y expresamente designado por la máxima autoridad del IDAC o por áreas delegadas para otorgar dichos permisos. Su divulgación o revelación no autorizada tiene un grave impacto en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización y está bajo la responsabilidad del Dueño de la Información.

Propiedad de IDAC: Salvo disposición legal o contractual que establezca lo contrario, todos los datos e información almacenada en o transmitida por medios digitales, analógicos, visuales, auditivos o gestuales, es propiedad de IDAC.

3.1 Pautas de Clasificación

Clasificación por defecto: La información que no tiene ni una designación como Pública o Confidencial, debe ser tratada como si fuera Interna hasta que el Dueño de la Información le designe una clasificación apropiada. Adicionalmente, la información que pertenece a terceros y que ha sido confiada al IDAC debe ser tratada como Confidencial a menos que una disposición legal o contractual indique lo contrario.

Reclasificación: La información designada como Confidencial permanecerá así hasta que sea especialmente desclasificada por el Dueño u otro directivo de IDAC en que se haya delegado esta responsabilidad propietaria. La única excepción involucra información que ha sido específicamente rotulada como Pública a partir de una cierta fecha o cuando tenga lugar un determinado evento.

3.2 Rotulación y manejo de información

Cada documento que ha sido designado como confidencial debe tener un proceso de comunicación o transmisión específico. Las versiones electrónicas de documentos deben tener el mismo proceso.

Toda salida impresa de computador designada como Confidencial debe estar de acuerdo con el proceso específico de manejo de ese documento. Su Dueño debe manejar todos los medios de almacenamiento legible por computador que contenga Información Confidencial.

Los Usuarios deben cubrir la Información Confidencial de sus escritorios o áreas de trabajo cuando personas no autorizadas estén cerca de ella.

De igual forma, los Usuarios deben bloquear su pantalla con contraseña, cerrar sesión o tomar acciones similares si personas no autorizadas están en posición de ver la pantalla de su computador.

Impresión remota: Las impresoras no deben ser desatendidas si se está imprimiendo o a punto de imprimir Información Confidencial. Se debe retirar todo el material impreso.

Las personas que manejan la impresora deben estar autorizadas para examinar la información que se imprime. La impresión no vigilada se permite sólo si es hecha en un área protegida tal que las personas que no están autorizadas para ver el material que está siendo impreso no puedan entrar.

Estas medidas deberán aplicarse también a fotocopadoras y escáneres, y no se deberá dejar fotocopias ni documentos sin retirar en bandeja de estos dispositivos.

3.3 Almacenamiento de la información confidencial

Contenedores seguros: Cuando no esté en uso, o cuando no esté bajo directa y continua supervisión visual, la información confidencial debe guardarse en un contenedor seguro tal como un gabinete o un escritorio con llave.

3.4 Reproducción de información confidencial

La reproducción de Información Confidencial, incluyendo la impresión de copias adicionales vía una impresora, no está permitida a menos que esté específicamente autorizada por su Dueño.

De igual forma, los extractos, resúmenes, traducciones, o derivados de la Información Confidencial no deben ser realizados a menos que el Dueño de la información lo haya aprobado previamente por escrito. Los Custodios pueden hacer copias de respaldo de información confidencial sin la aprobación específica del Dueño.

3.5 Eliminación de información confidencial

La Información Confidencial no puede ser eliminada de las instalaciones del IDAC a menos que haya una aprobación previa del Dueño de la información. Esto incluye la Información Confidencial almacenada en los discos de computadores, portátiles, impresiones, registros físicos en papel y similares. Se exceptúan las copias de respaldo autorizadas fuera del sitio.

3.6 Transporte de información confidencial

Transporte físico: El transporte físico de la Información Confidencial requiere el uso de un correo confiable tal como un personal de mensajería interna o servicios postales. Toda la Información Confidencial enviada por couriers (mensajeros) debe ser envuelta en un sobre opaco y sellado. Si se guarda alguna Información Confidencial en un medio legible por computador éste debe ser encriptado, cuando sea enviado vía Courier.

Transporte electrónico: El transporte electrónico de Información Confidencial es posible a través de mensajes de correo electrónico siempre y cuando el que envía esté usando el modo de encriptación. La Información Confidencial NO DEBE ser enviada ni transmitida por ningún medio electrónico a menos que sea en modo ENCRYPTADO, utilizando para ello una llave privada y una llave pública, conocida por los que tienen autorización para acceder a esa información Confidencial.

3.7 Destrucción de información confidencial

La destrucción de la información confidencial sólo se efectuará cuando se cumplan todas las condiciones siguientes:

- a) No exista un requerimiento legal o reglamentario de conservarla o el período de retención establecido en la legislación o regulación haya vencido.
- b) No sea propiedad del cliente.
- c) Haya perdido su valor administrativo, probatorio o constitutivo, o extintivo de derechos y que no haya desarrollado ni se prevea que vaya a desarrollar valores históricos.

El desecho en contenedores para reciclaje está prohibido. La Información Confidencial debe triturarse si está en papel.

La Información Confidencial residente en medios de almacenamiento electrónicos debe ser destruida reformateando o desmagnetizándola, si el medio será reutilizado por los sistemas del IDAC. La simple “eliminación” o “borrado” de la Información Confidencial almacenada en medios magnéticos no es suficiente ya que la información es aún recuperable. Si el medio no será reutilizado nuevamente, la información puede ser destruida con tijeras o puesta en un contenedor especial de destrucción de Información Confidencial.

4. Consecuencias de incumplimiento

El incumplimiento de las disposiciones contenidas tanto en la presente política como en los documentos relacionados se regirá por el Procedimiento Disciplinario del IDAC, la legislación y/o la normativa OACI, según apliquen.



Román Caamaño Vélez
Director General
Instituto Dominicano de Aviación Civil (IDAC)



Héctor Porcella Dumas
Subdirector General
Instituto Dominicano de Aviación Civil (IDAC)