DAN TIC 01

SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE LA INFORMACIÓN DE LA DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

HOJA DE VIDA

DAN TIC 01

"SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE LA INFORMACIÓN DE LA DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL"

ENMIENDA			PARTE AFECTADA DEL DOCUMENTO		DISPUESTO POR	
Nº	FECHA	ANOTADO POR	PÁRRAFO	PÁGINAS	DCTO.	FECHA

DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL
DEPARTAMENTO PLANIFICACIÓN

OBJ.: Aprueba Primera Edición de la DAN TIC 01 "Seguridad física para la protección de la información de la DGAC".

EXENTA Nº 01 /

SANTIAGO, 03 ENE. 2012

Con esta fecha se ha dictado la siguiente:

RESOLUCIÓN DE LA DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

VISTOS

a) Ley Nº 16.752, Orgánica de la DGAC.
b) Ley Nº 19.628, Sobre protección de la vida privada o protección de datos.
c) Decreto Supremo Nº 83 del 03.JUN.2004.
d) N. CH. 2777, Norma Chilena de Seguridad de la información.
e) ISO/IEC 27001, Sistemas de gestión de la seguridad de la información.
f) Resolución Exenta Nº 0873 del 05.AGO.2011.
g) Política Seguridad Física y del Ambiente aprobada por Resolución Exenta Nº 01278 del 15.NOV.2011.
h) DROF Departamento Tecnologías de Información y Comunicaciones.
i) DROF Departamento Planificación.
j) PRO ADM 02 "Estructura normativa de la DGAC".

CONSIDERANDO

La necesidad de establecer una normativa que regule materias de seguridad física para la protección de la información en la Dirección General de Aeronáutica Civil (DGAC).

RESUELVO

APRUÉBASE la Primera Edición de la Norma Aeronáutica DAN TIC 01 "Seguridad física para la protección de la información de la Dirección General de Aeronáutica Civil", la que entrará en vigencia treinta (30) después de la fecha de su promulgación.

Anótese y Comuníquese. **(FDO.) JAIME ALARCÓN PÉREZ, GENERAL DE AVIACIÓN, DIRECTOR GENERAL**
Lo que se transcribe para su conocimiento

DUNCAN SILVA DONOSO
CORONEL DE AVIACIÓN (A)
DIRECTOR DE PLANIFICACIÓN

DISTRIBUCIÓN:

PLAN "F".

ÍNDICE

DAN TIC 01

DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL
DEPARTAMENTO TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIONES

NORMA AERONÁUTICA

SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE LA INFORMACIÓN DE LA DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

Resolución Nº 01 del 03 de enero de 2012

I. PROPÓSITO

Prevenir los accesos físicos no autorizados e intromisiones en las instalaciones y evitar pérdidas de información en la Dirección General de Aeronáutica Civil (DGAC).

II. ANTECEDENTES

a) Ley Nº 16.752, Orgánica de la DGAC.
b) Ley Nº 19.628, Sobre protección de la vida privada o protección de datos.
c) Decreto Supremo Nº 83 del 03.JUN.2004.
d) N. CH. 2777, Norma Chilena de Seguridad de la información.
e) ISO/IEC 27001, Sistemas de gestión de la seguridad de la información.
f) Resolución Exenta Nº 0873 del 05.AGO.2011.
g) Política Seguridad Física y del Ambiente aprobada por Resolución Exenta Nº 01278 del 15.NOV.2011.
h) DROF Departamento Tecnologías de Información y Comunicaciones.
i) DROF Departamento Planificación.
j) PRO ADM 02 “Estructura normativa de la DGAC”.

III. MATERIA

Todos los activos de información de la Institución y la plataforma tecnológica que lo sustentan, así como los medios de almacenamiento que éstos usan, que residan en sus dependencias y/o en los proveedores de servicio o terceros, deben estar protegidos contra daño físico o hurto utilizando mecanismos de control de acceso físico que aseguren que únicamente el personal autorizado tiene acceso a los mismos

Esta norma es aplicable a todo el personal que realice funciones en la DGAC y quienes accedan a información sensible y/o a los activos de información en el desarrollo de sus tareas habituales.

CAPÍTULO 1
DEFINICIONES

SEGURIDAD FÍSICA
Aplicación de barreras físicas (puertas, muros, cerco electrónico, entre otros) y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los activos de información institucionales.

AMBIENTE
Comprende el conjunto de valores naturales, sociales y culturales existentes en un lugar y en un momento determinado, además de los relacionados con las variables que influyen directamente en el normal rendimiento de los activos de información de la institución, como ser, temperatura, humedad.

ACTIVO DE INFORMACIÓN
Se debe entender como la información propiamente tal, el medio donde está contenida, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, otros), los equipos o sistemas que la soportan, los procesos que la transforman y las personas que la utilizan, que posean valor para la organización.

ÁREA RESTRINGIDA
Lugar que administra información relacionada con procesos críticos y que sólo puede acceder personal debidamente autorizado.

CAPÍTULO 2

CONTROLES DE ACCESO

2.1 El acceso físico a los edificios, instalaciones y oficinas de las Unidades que componen la DGAC, debe ser restringido y controlado por medio de las siguientes medidas:

a) Los funcionarios deben registrar su entrada por medio de su credencial de identificación y portarla siempre en un lugar visible. De no ser así, deberá registrarse como visitante y portar la credencial correspondiente. Se procederá de la misma forma, para el caso de credenciales expiradas.

b) El personal externo o visitante deberá registrarse en la recepción de la DGAC y presentar su credencial de visitante al momento de ingresar a las instalaciones. También es obligatorio portarla en un lugar visible durante su permanencia en los edificios u oficinas. El otorgamiento de dicha credencial estará condicionado a la confirmación del funcionario de contacto correspondiente.

c) Deberá controlarse el ingreso a cobradores, vendedores, así como a personas que no dispongan de cita agendada con un funcionario de contacto.

d) Se deberá controlar a los funcionarios y visitantes respecto de elementos de carácter informático que portan al ingresar o salir de dependencias aeronáuticas.

e) No deberá permitirse el ingreso de cámaras de video, de fotografía, de grabación u otro elemento que representen riesgos al personal o al patrimonio de la DGAC, salvo previa autorización de la autoridad facultada.

2.2 Se deberán establecer áreas restringidas para las personas en las dependencias DGAC, que serán identificadas y protegidas, de acceso limitado y conforme al nivel de riesgo establecido, según lo disponga la autoridad facultada. Se emplearan mecanismos de identificación, registro y validación de accesos a las personas.

2.3 Las visitas que accedan en automóvil a unidades DGAC, podrán ser objeto de consultas sobre los elementos que portan, cuando existan antecedentes de riesgo para la seguridad informática de las instalaciones.

2.4 Control de personas durante la salida de las instalaciones de la DGAC

La salida de personal de las instalaciones y oficinas DGAC debe ser controlada por medio de las siguientes medidas:

a) Los empleados deben registrar su salida por medio de su credencial de identificación.

b) El personal externo o visitante deberá mostrar su credencial de visitante y registrar su salida de la unidad aeronáutica.

c) El personal de vigilancia deberá controlar, a la salida de unidades aeronáuticas, a las personas que porten o transporten mobiliario, equipo de cómputo/electrónico, herramientas de trabajo o documentos, sin que medie la autorización formal del área responsable del bien.

CAPÍTULO 3
SEGURIDAD EN LAS INSTALACIONES

3.1 Seguridad en las Oficinas

Las oficinas e instalaciones institucionales deben cumplir con los siguientes controles:

a) Las áreas restringidas deben ser debidamente controladas para evitar el acceso público.

b) Los equipos departamentales de fotocopiado, impresión o fax deberán estar preferentemente dentro de áreas restringidas y bajo la supervisión de personal autorizado. Nunca en lugares donde se pueda comprometer la seguridad de la información.

c) Las puertas y ventanas deben permanecer cerradas en ausencia del personal que labora en las oficinas, salvo expresa autorización en contrario.

d) El uso de equipo fotográfico, de video o de audio grabación solamente está permitido en las áreas autorizadas.

e) Cuando se establezca un edificio o dependencia que contenga equipos de procesamiento crítico de datos, debe ser estéril respecto a la seguridad, en lo posible con paredes de construcción sólida y las puertas protegidas para acceso no autorizado.

f) Se deberán establecer barreras físicas que eviten toda vulnerabilidad de las dependencias y la contaminación del ambiente causada por terremoto, fuego, inundación u otro tipo de evento adverso.

g) Las dependencias deberán contar con puertas contrafuego, dispositivos de alarma contra incendio y cierre automático.

3.2 Áreas de carga y descarga

3.2.1 Las áreas de carga y descarga deberán ser controladas y vigiladas con circuito cerrado de televisión, con la finalidad de evitar el acceso de personas no autorizadas y situadas en un sector que no afecte la seguridad de los activos de información críticos de la Institución.

3.2.2 Se deberá controlar el ingreso de equipos o materiales a las instalaciones aeronáuticas a fin de prevenir posibles eventos adversos a los activos de información críticos de la Institución. Cada unidad deberá establecer el procedimiento interno para implementar estas medidas.

3.2.3 El transporte de activos de información institucional fuera de las instalaciones deberá ser autorizada por la Jefatura de unidad involucrada.

3.3 Seguridad de plataformas tecnológicas

3.3.1 Los elementos o equipos constitutivos de plataformas tecnológicas deberán estar situados y protegidos ante eventos adversos o accesos no autorizados de personas.

3.3.2 Todos los equipos destinados al procesamiento y almacenamiento de información deberán estar ubicados dentro de instalaciones (Sala de servidores, oficinas) y contar con mecanismos de protección.

3.4 Equipo de procesamiento de información

3.4.1 Las instalaciones, equipos y accesorios para el procesamiento de información utilizados por el personal de la DGAC para el desarrollo de sus funciones, deberán ser conservadas y utilizadas para los fines institucionales, adoptando medidas para garantizar su uso y cuidado.

3.4.2 Se deberán monitorear las condiciones ambientales, tales como temperatura y humedad, que pudiera afectar adversamente los activos de información.

3.4.3 No está permitido la intervención de los activos de información por parte de funcionarios que no sean del Departamento TIC o autorizados por este.

3.4.4 En caso de existir activos de información de carácter confidencial, éstos se deberán proteger, a objeto de minimizar el riesgo de fuga de información o intrusión en los sistemas.

3.5 Energía eléctrica

3.5.1 Los equipos de procesamiento de información deberán estar protegidos ante fallas en el suministro de energía eléctrica. Aquellos equipos asociados a los procesos críticos de la Institución deben contar con:

a) Múltiples fuentes de alimentación de electricidad, fuente ininterrumpida de poder (UPS) y generador de energía de respaldo.

b) Los UPS y generadores de energía de respaldo deberán ser probados y revisados periódicamente, de acuerdo a las especificaciones del fabricante, por el departamento competente, con la finalidad de que la continuidad operativa

institucional no se vea afectada. A su vez, deberá mantenerse un registro de revisiones y pruebas realizadas.

c) Se deberán instalar interruptores de emergencia de corte de energía cercano a las salidas de emergencia en oficinas e instalaciones donde se encuentra el equipo de procesamiento de información, para facilitar el cierre del paso de corriente.

d) Se deberá disponer de un sistema de iluminación de emergencia en caso de falla del sistema principal.

e) El suministro de fuerza electromotriz deberá ser compatible con las necesidades del equipamiento instalado y protegido ante fallas del suministro.

3.5.2 Se deberá aplicar protección contra las variaciones de voltaje e interferencia eléctrica en todas las instalaciones donde existan activos de información.

CAPÍTULO 4

SEGURIDAD EN EL PROCESAMIENTO DE LA INFORMACIÓN

4.1 El equipamiento para el procesamiento de información y la plataforma tecnológica asociada debe contar con programas de mantenimiento para asegurar su correcto funcionamiento y disponibilidad.

4.2 El mantenimiento deberá llevarse a cabo de acuerdo a las especificaciones del fabricante y solamente con personal autorizado.

4.3 El área responsable del mantenimiento deberá llevar un registro de las fallas o funcionamiento subestandard, para determinar las medidas preventivas o correctivas que correspondan.

4.4 En caso que el mantenimiento se efectúe fuera de las dependencias aeronáuticas, deberá ser autorizado por la autoridad competente y notificada al personal de vigilancia de la dependencia para su control.

4.5 Procesamiento de información fuera de la DGAC

4.5.1 La instalación y uso de equipamiento para el procesamiento de información e infraestructura tecnológica para el manejo de información fuera de la DGAC debe ser aprobado por la autoridad correspondiente, dejando registro en su bitácora u hoja de vida.

4.5.2 Los equipos que sean llevados fuera de las instalaciones de la DGAC deberán ser protegidos según instrucciones del fabricante y utilizados para los fines propios, sin afectar los intereses y patrimonio institucional.

4.6 Reutilización de los equipos de procesamiento de la información

4.6.1 El Departamento TIC deberá considerar un procedimiento para la disposición y reutilización de un equipo de procesamiento de información, así como para la destrucción apropiada de datos, de acuerdo a la legislación vigente.

4.6.2 Se deberán chequear los ítems del equipo de procesamiento de información que contiene medios de almacenamiento para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación

4.6.3 Los dispositivos que contienen información sensible deberán ser físicamente destruidos o se deberán destruir, borrar o sobre-escribir, utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.

4.6.4 Los dispositivos que contienen información sensible pueden requerir una evaluación del riesgo para determinar si los ítems deberán ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

CAPÍTULO 5

CONFIDENCIALIDAD

5.1 Las instalaciones y datos informáticos existentes y generados por la Institución en cualquier soporte físico o lógico, dispositivos o soportes de dominio son de propiedad de la Dirección General de Aeronáutica Civil, en conformidad a la Ley, salvo se estipule en contrario, prohibiéndose su uso no autorizado.

5.2 Los funcionarios o quienes tengan acceso a las áreas restringidas, mantendrán absoluta confidencialidad de la información que tomen conocimiento en el ejercicio de sus funciones, de la arquitectura física y lógica de las instalaciones que visiten, y de toda información de datos informáticos contenidos en hardware, software, fireware y/o de redes, accesos remotos o telecomunicaciones.

5.3 No se permite el acceso remoto, ni el telemando a distancia de los dispositivos informáticos instalados en áreas restringidas de la DGAC, salvo expresa autorización.

5.4 Obligaciones de notificación

5.4.1 Los funcionarios deben notificar a su Jefatura, tan pronto sea posible, de cualquier incidente que afecte a los activos de información o que pueda constituir una vulnerabilidad a la arquitectura física o lógica de los mismos.

5.4.2 Se mantendrá un registro de incidentes de seguridad de la información a cargo del encargado de Seguridad de la Información de la institución, con indicación de las fallas y medidas correctivas y preventivas.

5.4.3 La infracción a las disposiciones al presente procedimiento, será sancionada de la forma establecida en el Estatuto Administrativo.

5.5 Obligaciones de capacitación, revisión y actualización

5.5.1 Los programas de capacitación dirigidos al personal deben considerar materias de seguridad de la información y el uso adecuado de los activos tecnológicos.

5.5.2 Esta capacitación considerará particularmente el desarrollo de habilidades en el personal, para operar y enfrentar situaciones de contingencia. Los programas de inducción al personal nuevo comprenderán las materias señaladas en esta norma.

5.5.3 Se elaborará un estudio anual de las prácticas de seguridad de información y la actualización de la matriz de riesgo de seguridad, para el examen del nivel de cumplimiento de la presente norma, del Decreto Supremo Nº 83 Incluir en los antecedentes (MINSEGPRES) y de la Norma ISO27001 sistema de gestión de seguridad de la información, como de la implementación de medidas de mejora continua en esta materia.

5.5.4 El Comité de Seguridad de la Información y el Encargado de Seguridad se reunirán anualmente para la revisión y actualización de la presente norma.

IV. VIGENCIA

La presente Norma Aeronáutica entrará en vigencia treinta (30) días después de la fecha de la resolución aprobatoria.