Ministerio de Defensa
Unidad de Auditoria Interna

MD Nº 22101 | 16
UAI Nº 355 | 16

INFORME DE AUDITORÍA Nº 042/2016
MINISTERIO DE DEFENSA
ESTADO MAYOR GENERAL DE LA FUERZA AÉREA
DIRECCIÓN GENERAL DE COMUNICACIONES E INFORMÁTICA
DIRECCIÓN DE INFORMÁTICA POLÍTICA DE SEGURIDAD

Tabla de Contenidos

Ministerio de Defensa
Unidad de Auditoria Interna

Informe Ejecutivo

INFORME DE AUDITORÍA Nº 042/2016
MINISTERIO DE DEFENSA
ESTADO MAYOR GENERAL DE LA FUERZA AÉREA
DIRECCIÓN GENERAL DE COMUNICACIONES E INFORMÁTICA
DIRECCION DE INFORMÁTICA POLÍTICA DE SEGURIDAD

Objetivo

Evaluar la puesta en práctica de la Política de Seguridad de la Información en el ámbito de LA DIRECCIÓN GENERAL DE COMUNICACIONES E INFORMÁTICA DE LA FUERZA AÉREA ARGENTINA, en cumplimiento a los lineamientos estipulados por Disposición 01/15 ONTI.

Conclusión

La Dirección General de Comunicaciones e Informática aplica lineamientos definidos para todo el ámbito de la Fuerza cumplimentando lo establecido en la Disposición 01/15 ONTI, a través de la implementación del Manual de Políticas y Normas denominado "MAPG N° 22"

Con base en los Puntos de Control establecidos en el Alcance de esta Auditoría, *Clausula 12* se pudo constatar que el "*Departamento Seguridad Informática*" contempla lineamientos de seguridad, minimizando riesgos y aplica los controles necesarios en cada procedimiento para mantener la Seguridad en las Operaciones.

Dr. Pablo L. Lestingi
Auditor Interno
MINISTERIO DE DEFENSA

BUENOS AIRES, octubre 2016

Ministerio de Defensa
Unidad de Auditoria Interna

Informe Analítico

INFORME DE AUDITORIA Nº 042/2016
MINISTERIO DE DEFENSA
ESTADO MAYOR GENERAL DE LA FUERZA AÉREA
DIRECCIÓN GENERAL DE COMUNICACIONES E INFORMÁTICA
DIRECCION DE INFORMÁTICA POLÍTICA DE SEGURIDAD

Objetivo

Evaluar la puesta en práctica de la Política de Seguridad de la Información en el ámbito de LA DIRECCIÓN GENERAL DE COMUNICACIONES E INFORMÁTICA DE LA FUERZA AÉREA ARGENTINA, en cumplimiento de los lineamientos estipulados por Disposición Nº 01/15 ONTI.

Alcance

La auditoría se circunscribió a la Clausula 12 – "*Seguridad en las Operaciones*" de la Disposición Nº 01/15 ONTI en la Dirección de Informática - Departamento Seguridad Informática.

Tareas realizadas

Las tareas se desarrollaron durante el mes de Septiembre y Octubre del presente año, en las instalaciones de la Dirección General de Comunicaciones e Informática de la Fuerza Aérea Argentina, "DIRECCION DE INFORMATICA", en el Edificio Cóndor, de acuerdo con las Normas de Auditoría Interna Gubernamental aprobadas por Resolución SGN Nº 152/02, aplicándose algunas de los procedimientos allí enunciados.

Dentro de las actividades realizadas, se llevaron a cabo entrevistas con autoridades del lugar y jefes de área, análisis de documentación solicitada y verificación de procedimientos por medio de inspecciones oculares en el Centro de Cómputos.

A continuación se exponen los puntos de control relevantes en que se focalizó el análisis, según lo establecido en el Instructivo de Trabajo Nº 6/2015 – GNYPE

1. Procedimientos Generales Operativos

   La Dirección de Informática realizó un estudio denominado "Análisis y Gestión de Riesgos" en el cual define:

   - Inventario de Activos (hardware–software-base de datos) y su Valoración
   - Amenazas

- Identificación de Controles
- Determinación de impacto frente a las diferentes amenazas
- Calculo de Riesgo

Como resultado de este análisis, se elaboran Planes, Procedimientos y se implementan herramientas informáticas con el objetivo de minimizar los riesgos.

Dentro de lo requerido en este punto se pudo constatar lo siguiente:

- Acuerdos de confidencialidad con los usuarios.
- Restricción en el uso de software para conectar un equipo.
- Soporte y mesa de ayuda
- Plan de contingencia y recuperación en caso de fallas.
- Mantenimiento de equipos.
- Monitoreo de procesamiento y comunicaciones.
- Procedimiento de Backup y contingencia de Base de Datos.
- Gestión de incidentes y notificaciones.
- Uso del correo electrónico institucional.

2. Protección contra malware

La Circular Informática Nº 02/16 "Utilización del servicio de internet en la Fuerza Aérea Argentina" especifica el uso de Software de control de Aplicaciones, IPS (intrusión prevention system), antivirus, antispyware, antispam.

Asimismo la Circular Nº 1/15 "Licencias y uso de software" específica las configuraciones básicas que debe tener un equipo antes de ser conectado a la Red de Fuerza Aerea.

3. Resguardo Backups

El procedimiento de backup de servidores e información de los usuarios, se realiza a diario en Discos Externos y Cinta LTO 5 y finalmente se resguardan en la caja fuerte ignífuga. Asimismo, se cuenta con un centro de cómputos alternativo (Centro Asistencial Retiro: Sanidad) con la información crítica de la FAA y se posee una biblioteca virtual con el software necesario para restablecer los servicios.

4. Registro y monitoreo

Se mantiene registro de las actividades, excepciones y eventos de seguridad mediante:

- Planilla incidente informáticos.
- Consultas y reportes a través del sistema **lechuza.condor.faa** (identificación de los usuarios, identidad del equipo y la ubicación, permisos asignados)
- Consulta y reportes a través del sistema **SARG** (squid analysis report generator) de todos los log (registro de actividad de un sistema)

5. Control de Software

Los cambios se registran según lo establecido en la Circular Nº 32 "Cambios en las operaciones" y la implementación de software se lleva a cabo según las Circulares Nº 29 "Implementación de software en ambientes productivos" y Circular Nº 31 "Implementación de sistemas informáticos"

El acceso al ambiente de producción se encuentra restringido a todos los programadores o analistas de desarrollo y mantenimiento de aplicaciones mediante:

- Estación de trabajo
- IP del equipo
- Usuario del sistema
- Permisos de lectura, escritura y ejecución en el sistema.

6. Administración de vulnerabilidades

Se ejecutan diariamente escaneos de vulnerabilidades con diferentes herramientas como NESSUS, VEGA y NMAP, según los resultados, se informa problemas y soluciones.

7. Consideraciones sobre la auditoria de sistemas

Se informa al Organismo / Unidad los requerimientos de Auditoria (vía correo aeronáutico) en base a:

- Plan de Auditoría de la Inspectoría General (Guía Informática).
- Hallazgos en Inspecciones de años anteriores.

Marco Normativo

La normativa considerada para las actividades de Tecnología de la Información (TI) es:

- Decisión Administrativa (DA) N° 669/2004 de Jefatura de Gabinete. Establece que los Organismos del Sector Público Nacional deben dictar o adecuar sus Políticas de Seguridad de la Información, conformar el Comité de Seguridad de la Información con sus funciones y asignar las responsabilidades sobre la Seguridad de los Sistemas de Información.

- Disposición Nº 01/15 de la ONTI "Política de Seguridad de la Información Modelo"
- Circular SIGEN N° 2/2012 – SGN – Aspectos Organizacionales basados en la Resolución Nº 48/2005 - Normas de Control Interno para Tecnología de la Información.
- Instructivo de Trabajo Nº 6/2015 - GNYPE - Revisión de la Política de Seguridad de la Información según modelo aprobado por Disposición Nº 1/2015 ONTI

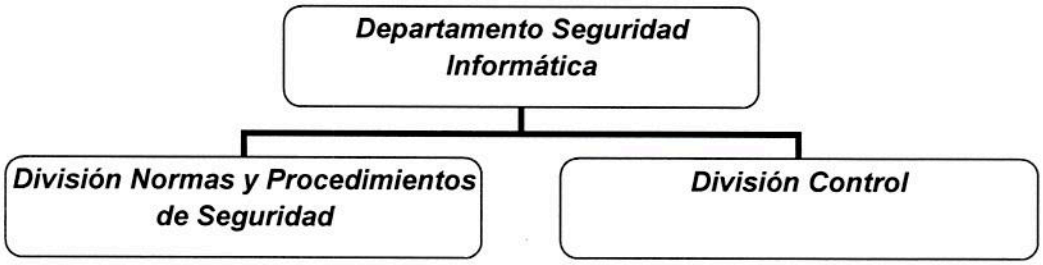
Marco de Referencia

En el Anexo I del presente Informe se resumen brevemente los antecedentes de la Dirección General de Comunicaciones e Informática y en el Anexo II se incluye el organigrama de la estructura actual de la Dirección de Informática.

LA DIRECCIÓN DE INFORMÁTICA está conformada por tres departamentos, a saber:

- Seguridad Informática
- Desarrollo y Mantenimiento de Sistemas
- Procesamiento y Servicios

El trabajo se focalizó sobre el **Departamento Seguridad Informática**, con una dotación de 7 efectivos, distribuidos según Manual Orgánico de la Dirección de Informática (MAPO 72 Edición 2013), a su vez conformado por 2 divisiones. A continuación se presenta el organigrama del sector.



Tiene como tarea "*Determinar las políticas, normas y procedimientos de seguridad de los sistemas informáticos y las redes de transmisión de datos en estado de producción de la Fuerza, y asegurar el cumplimiento de las actividades derivadas de su aplicación*", siendo sus funciones:

- *Entender en el establecimiento de la normativa que rige y regula el desarrollo de la actividad del área a nivel institucional, en base a las*

necesidades y particularidades de la Fuerza, y conforme lo establecido a nivel nacional para el ámbito de la Administración Pública.

- *Entender en la determinación de los sistemas de control tendientes a detectar vulnerabilidades en los sistemas informáticos y las redes de transmisión de datos en estado de producción de la Fuerza.*

- *Entender en la adopción de las medidas y establecer los recursos que se determinen necesarios y suficientes para dar cumplimiento a la normativa vigente, para resguardar la información que se almacena, procesa y/o transmite con recursos informáticos en el ámbito institucional.*

- *Participar del Plan Anual de Inspecciones que conduce la Inspectoría General, verificando la correcta aplicación de la normativa vigente en el área y la correspondiente explotación de recursos asignados al efecto.*

- *Entender en el establecimiento de las relaciones institucionales y extra institucionales que se consideren necesarias para mejorar la actividad del área en aspectos doctrinarios y tecnológicos.*

- *Entender en el análisis y propuesta de la incorporación de nuevas tecnologías o prácticas de seguridad informática, para su aplicación a nivel institucional.*

- *Entender en la aplicación de los lineamientos establecidos para su área de competencia en las circulares informáticas.*

- *Desarrollar, además, todas las otras funciones que surjan de su tarea, las complementarias de la misma y las necesarias para su administración interna.*

De acuerdo a las entrevistas realizadas y a la documentación analizada, las tareas que realiza la Dirección son:

- Monitoreo y seguridad de la red que accede a Internet de, aproximadamente, 1.700 usuarios.
- Monitoreo y seguridad de la red intranet de, aproximadamente, 1.100 usuarios.
- Supervisión de políticas en servidor antivirus de ambas redes.
- Supervisión de políticas de seguridad en servidores de e-mail de ambas redes (intranet e Internet) de 3.400 cuentas de correo.
- Supervisión de políticas en aplicación de filtro de contenidos de navegación a Internet.

Ministerio de Defensa
Unidad de Auditoria Interna

- Asesoramiento a los responsables informáticos de las Unidades de la Fuerza Aérea (FAA) respecto de la política y medidas de seguridad informática.
- Supervisión de la instrumentación de las medidas de seguridad en la red LAN de la FAA.
- Supervisión de la instrumentación de las medidas de seguridad en la red WAN de la FAA.
- Supervisión de la política y medidas de seguridad informáticas en el sitio Web de la FAA.
- Análisis de Logs de los servidores de FW y en producción.
- Realización de auditorías en las unidades de la FAA en coordinación con la Inspectoría General.

Conclusión

La Dirección General de Comunicaciones e Informática aplica lineamientos definidos para todo el ámbito de la Fuerza cumplimentando lo establecido en la Disposición 01/15 ONTI, a través de la implementación del Manual de Políticas y Normas denominado "MAPG N° 22"

Con base en los Puntos de Control establecidos en el Alcance de esta Auditoría, *Clausula 12* se pudo constatar que el "*Departamento Seguridad Informática*" contempla lineamientos de seguridad, minimizando riesgos y aplica los controles necesarios en cada procedimiento para mantener la Seguridad en las Operaciones.

Dr. Pablo L. Lestingi
Auditor Interno
MINISTERIO DE DEFENSA

BUENOS AIRES, octubre 2016

Ministerio de Defensa
Unidad de Auditoria Interna

ANEXO I

Dirección General de Comunicaciones e Informática

Nació como Dirección General de Estadística en 1944 y en 1965 pasó a denominarse Centro de Cómputos de la FAA, desde 1970 cambió su denominación a Departamento de Computación Automática de Datos (SICAD) y Dirección de Informática desde 1990.

El Departamento Seguridad Informática fue creado en 2003, e incluido en el Manual Orgánico de la Dirección de Informática (MAPO 72 Edición 2003)

La Dirección General de Comunicaciones e Informática como tal fue creada en el año 2011 por Resolución MD Nro. 1633/2010 "MATRIZ COMÚN ESTRUCTURA ORGÁNICA FUNCIONAL FF.AA".

En cuanto a la Dirección de Informática tiene como **Misión** la de: *"Planificar a corto plazo, desarrollar, ejecutar y controlar los sistemas informáticos y las redes de transmisión de datos de la Fuerza Aérea, asegurando el comando y control, a fin de contribuir con las tareas de la Dirección General de Comunicaciones e Informática".*

Sus **funciones** son:

1. *Entender en la planificación de las etapas del ciclo de vida de aquellos sistemas informáticos que se hayan establecido para contribuir a las funciones de gobierno de la Fuerza Aérea (operativas, administrativas y de gestión), realizando la evaluación y selección de recursos que mejor se adecuen a ese propósito.*
2. *Entender en la ejecución de las etapas del ciclo de vida de aquellos sistemas informáticos que se lleven a cabo con recursos del Organismo o aquellos que específicamente se determinen y, cuando corresponda, determinar la viabilidad de los cambios requeridos a sistemas en producción.*
3. *Entender en el desarrollo de las políticas informáticas que se determinen para todo el ámbito institucional y controlar su aplicación, coordinando la actividad de los responsables informáticos de los Organismos o Unidades de la Fuerza.*
4. *Entender en la implementación de la normativa necesaria para regular la ejecución de la actividad informática en la Fuerza, conforme las disposiciones establecidas para el ámbito de la Administración Pública Nacional y/o a las necesidades de orden institucional, controlando su aplicación.*

5. *Entender en todos los aspectos de seguridad informática a nivel institucional para garantizar la confidencialidad, integridad y disponibilidad de los datos y de la in-formación que se procesa o transmite mediante la utilización de recursos informáticos.*
6. *Entender en la ejecución de las inspecciones y/o auditorías de control interno en el área informática, en la forma y en las oportunidades que requiera la Inspectoría General de la Fuerza Aérea Argentina.*
7. *Entender en el control de la información obtenida del empleo de recursos informáticos para que se utilice de acuerdo a las finalidades previstas, sirva a los intereses de sanas prácticas administrativas y sea explotada conforme al marco legal, reglamentario y de seguridad vigente en la Fuerza.*
8. *Entender en la planificación y ejecución de los programas de perfeccionamiento y capacitación del personal de la especialidad y de aquel que específicamente se determine, para contribuir con el desarrollo de la actividad a nivel institucional.*
9. *Entender en el fomento de las actividades de investigación y explotación de tecnologías, conforme a la evolución o los cambios que experimente el segmento informático, contribuyentes con el progreso y el desarrollo de la Fuerza en el área, y que se correspondan con la normativa vigente.*
10. *Entender en la administración de las redes de transmisión de datos y los servidores que se determinen.*
11. *Entender en el procesamiento digital de la información que se determine con los medios asignados y conforme a la normativa vigente.*
12. *Entender en el resguardo de la información digital que se procesa en el ámbito del Organismo, y aquella que específicamente se determine, con los medios asignados y conforme a la normativa vigente.*
13. *Asistir a todos los Organismos y Unidades de la Fuerza en aspectos relacionados con la adquisición, contratación y/o explotación de bienes, insumos y/o servicios de carácter informático.*
14. *Desarrollar todas las otras funciones que surjan de su misión o tarea, las complementarias a la misma y las necesarias para su administración interna.*

ANEXO II

ESTRUCTURA ORGÁNICA DE LA DIRECCIÓN