

| | | |
|--|---|--------------|
|  | | Página 1 / 7 |
| AUDITORÍA DE GESTIÓN ADUANERA | <p style="text-align: center;">Asunto</p> INFORME SOBRE ASPECTOS ORGANIZATIVOS DE LOS SISTEMAS DE INFORMACIÓN. | |

INFORME DE AUDITORIA DE CUMPLIMIENTO N° 40 / 2016

AL : Econ. Gustavo J. Sotto, Jefe
AUDITORÍA DE GESTIÓN ADUANERA

DE : Lic. Roberto Molinas, Auditor Informático
AUDITORÍA DE GESTIÓN ADUANERA

OBJETO Informar resultado de las entrevistas realizadas para la evaluación de los Aspectos Organizativos de los Sistemas de Información.

FECHA : 28 de octubre del 2016.

A los efectos de dar cumplimiento de la resolución DNA N° 612 de fecha 22 de octubre del 2015, por la cual se aprueba el Plan de Trabajo Anual y Cronograma de Actividades para el Ejercicio Fiscal 2016 de la Auditoría de Gestión Aduanera, en carácter de Auditor Informático, presento a ustedes el Informe siguiente.

El informe es emitido para dar conocimiento sobre las condiciones en las que se encuentran los Aspectos Organizativos de los Sistemas de Información.

I. Objetivo

El objetivo de los controles realizados en nuestra revisión incluye:

Desarrollar una Auditoría Informática dentro de la Administración del sistema SOFIA enfocada a la Aspectos Organizativos de la Seguridad de la Información, utilizando herramientas y técnicas actualizadas de auditoría informática para determinar posibles falencias y proporcionar alternativas de solución.

En este caso el marco de referencia utilizado para el trabajo corresponde al Código de Buenas Prácticas para la gestión de la seguridad de la información ISO 27002-2013, abarcando los siguientes Dominios – Objetivos de Control y Controles:

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

- Organización Interna
 - Asignación de responsabilidades para la seguridad de la información.
 - Segregación de tareas.
 - Contacto con autoridades.
 - Políticas de uso de dispositivos para movilidad.
 - Teletrabajo.



| | | |
|--|---|--------------|
|  Aduana Paraguay | | Página 2 / 7 |
| AUDITORÍA DE GESTIÓN ADUANERA | Asunto INFORME SOBRE ASPECTOS ORGANIZATIVOS DE LOS SISTEMAS DE INFORMACIÓN. | |

II. Alcance

El proceso de Auditoría Informática se realizará dentro de la Administración SOFIA en todos los departamentos, como también en todos los sectores, áreas y divisiones vinculados con la información sensible procesada.

III. Metodología

El trabajo de auditoría se ha realizado dentro de un marco metodológico basado en el estándar ISO 27000, el cual nos permite enfocar en aspectos puntuales los trabajos a realizar; este ordenamiento es realizado mediante los dominios, objetivos de control y controles correspondientes.

Como herramienta de relevamiento, se han realizado entrevistas a los involucrados dentro de la Administración SOFIA, arrojando como resultado el estado actual del funcionamiento y aplicación de todo lo relacionado a seguridad operativa.

El informe presenta los resultados por medio de 3 situaciones:

- Nivel de Cumplimiento (**Alto, Medio, Bajo**)
- Riesgo (**Alto, Medio, Bajo**)
- Situación Actual
- Recomendaciones

En el **anexo I**, se citan todos los puntos con sus correspondientes descripciones y recomendaciones para mitigar los riesgos encontrados.

En el **anexo II**, se expone la situación actual de los dominios de manera gráfica.



| | | |
|--|---|--------------|
|  | | Página 3 / 7 |
| AUDITORÍA DE GESTIÓN ADUANERA | <p style="text-align: center;">Asunto</p> INFORME SOBRE ASPECTOS ORGANIZATIVOS DE LOS SISTEMAS DE INFORMACIÓN. | |

ANEXO I

1 POLITICAS - ASIGNACION DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACION.

1.1 Documentación y procedimientos de operaciones.

- Nivel de Cumplimiento: **MEDIO**
- Nivel de Riesgo: **ALTO**
- Situación Actual
 - a. En la actualidad se cuenta con unos "Manuales de Descripción de Puestos y Perfiles" en los cuales se detallan las competencias básicas requeridas para cada puesto como también los conocimientos.
 - b. Esta documentación entro en vigencia en el año 2012 pero ya se establecia en la Resolución N° 695 del 13 de octubre del 2010, y presenta competencias muy genéricas en algunas especificaciones, como así también la NO EXCLUSION a un puesto por falta de conocimiento sobre puntos criticos.
- Recomendaciones
 - a. Se deben actualizar los Manuales de Descripción de Puestos y Perfiles según la competencia real a cada puesto teniendo como resultado los siguientes puntos:
 - i. Evitar fuga de personal, ya que el perfil del candidato no corresponde a uno técnico y capacitado para las necesidades del área.
 - ii. Se evita personal ocioso o que no pueda ser asignado a determinadas tareas por falta de competencia.
 - iii. Poder contar con una base real sobre la cual se puedan realizar evaluaciones, capacitaciones, mejorando de esta manera al personal con un mayor y más sólido conocimiento para el desempeño de sus funciones.

1.2 Segregación de Funciones

- Nivel de Cumplimiento: **MEDIO**
- Nivel de Riesgo: **MEDIO**
- Situación Actual
 - a. La segregación de funciones está establecida en los Manuales de Descripción de Puestos y Perfiles donde se establece claramente las responsabilidades de cada empleado.
 - b. No existe un registro de todas las tareas realizadas para corroborar posteriormente que no se estén o solapando responsabilidades o deslindando las mismas.



- c. Otra situación que perdura es la existencia de dos áreas que realizan despliegue ya que actualmente se encuentra en fase de migración los aplicativos, apuntando de esta manera a la centralización de una sola tecnología.

- **Recomendaciones**

- a. Realizar un registro formal de las operaciones realizadas por cada empleado apoyadas en los pedidos a ser ejecutados de manera a controlar que tareas están realizando y si están asignados o no a las mismas.
- b. Establecer un listado de todos los aplicativos que deben ser migrados y presentarlos bajo un cronograma de trabajo, estimando de esta manera el momento de regularización de la tarea de despliegue.

1.3 Contacto con las autoridades

- Nivel de Cumplimiento: **BAJO**

- Nivel de Riesgo: **MEDIO**

- **Situación Actual**

- a. No se realizan reuniones o contacto apropiado con las autoridades pertinentes.
- b. Si se realizan a nivel de Jefatura.

- **Recomendaciones**

- a. Se debería mantener contacto apropiado con las autoridades relevantes pertinentes mediante reuniones en las cuales se puedan tratar temas de diferente índole.

1.4 Política de uso de dispositivos móviles

- Nivel de Cumplimiento: **MEDIO**

- Nivel de Riesgo: **BAJO**

- **Situación Actual**

- a. No existe una política sobre dispositivos móviles.

- **Recomendaciones**

- a. Se debe tener una política y medidas de seguridad de soporte a ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles. Esta política contendrá requisitos de protección física, controles de acceso, técnicas criptográficas, respaldos y protección antivirus.
- b. Se debe tener un especial cuidado para asegurar que la información de negocio no se comprometa cuando se usan dispositivos de informática móvil como:
 - i. Portátiles
 - ii. Teléfonos móviles



| | | |
|---|--|---------------------|
|  | | <p>Página 5 / 7</p> |
| <p>AUDITORÍA DE GESTIÓN ADUANERA</p> | <p style="text-align: center;">Asunto</p> <p style="text-align: center;">INFORME SOBRE ASPECTOS ORGANIZATIVOS DE LOS SISTEMAS DE INFORMACIÓN.</p> | |

1.5 Teletrabajo

- Nivel de Cumplimiento: **MEDIO**
- Nivel de Riesgo: **ALTO**
- Situación Actual
 - a. No se cuenta con políticas, planes operacionales y procedimientos para las actividades de teletrabajo.
- Recomendaciones
 - a. La posibilidad de realizar actividades de teletrabajo solamente debería poder realizarse si se han satisfecho las disposiciones y controles de seguridad apropiados y se cumple la política de seguridad de la organización. El teletrabajo debe estar debidamente autorizado y controlado.
 - b. El lugar de teletrabajo debe estar debidamente protegido contra:
 - i. El robo o equipo.
 - ii. La distribución no autorizada de información.
 - iii. El acceso remoto no autorizado.
 - iv. El mal uso de los dispositivos.

Sin otro particular, me despido de usted atentamente.

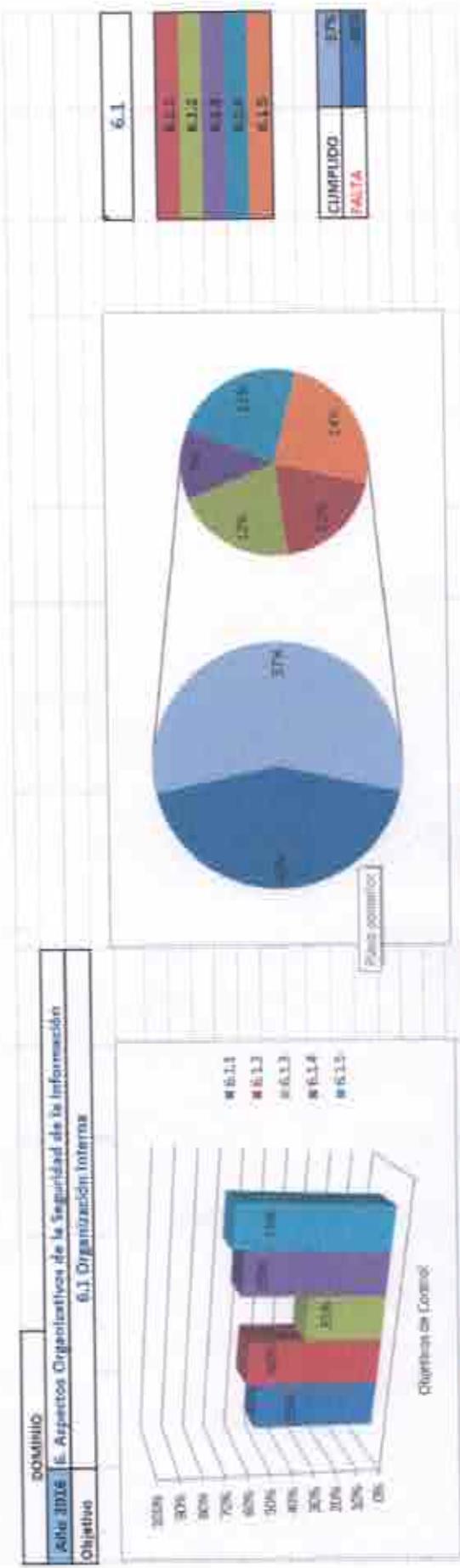
Lic. Roberto Molinas
Auditor de Sistemas

.....
Lic. Roberto Molinas
Auditor Informático – AGA

ANEXO II (Gráfico de Cumplimiento)

Aspectos Organizativos de la Seguridad de la Información

- Organización Interna

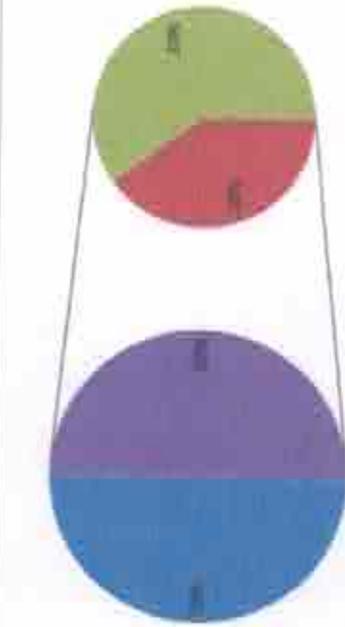
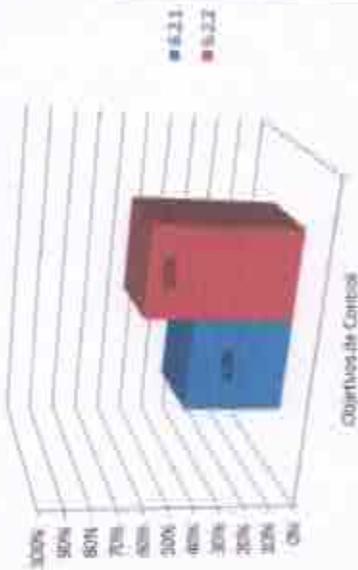


| Objetivos de Control | Comentarios |
|--|-------------|
| 6.1.1. Asignación de responsabilidades para la seguridad de la información | |
| 6.1.2. Seguridad de acceso | |
| 6.1.3. Control de la actividad | |
| 6.1.4. Control de la actividad de seguridad | |
| 6.1.5. Seguridad de la información de la gestión de la información | |



Dispositivos para Movilidad y Teletrabajo

Objetivo 6.2 Dispositivos para Movilidad y Teletrabajo



| | |
|----------|------|
| 6.2 | |
| 6.2.1 | |
| 6.2.2 | |
| CUMPLIDO | 100% |
| FALTA | 0% |

Objetivos de Control 6.2.1 Realidad de uso de dispositivos para movilidad
6.2.2 Teletrabajo