| Aduana | |
|---|---|
| AUDITORÍA DE GESTION ADUANERA | Asunto<br>INFORME SOBRE LA EVALUACION DE LA SEGURIDAD OPERATIVA. |

## INFORME DE AUDITORIA DE CUMPLIMIENTO N° 11 / 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 la Auditoria realizada sobre la Evaluación de la Seguridad Operativa.

**FECHA** : 11 de abril 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 Auditoria 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 las Políticas, Procedimientos y Ejecución de las medidas de la Seguridad Operativa.

## I. Objetivo

El objetivo de los controles realizados en nuestra revisión incluye:

Desarrollar una Auditoria Informática dentro de la Administración del sistema SOFIA enfocada a la Seguridad Operativa, utilizando herramientas y técnicas actualizadas de auditoria 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:

**SEGURIDAD OPERATIVA**

- Responsabilidades y Procedimientos de operación
  - Documentación de procedimientos de operación.
  - Gestión de Cambios.
  - Gestión de Capacidades.
  - Separación de entornos de desarrollo, prueba y producción.

RECIBIDO 11 ABR. 2016

- Registro de actividad y supervisión
  - Registro de gestión de eventos de actividad.
  - Protección de los registros de información.
  - Registros de actividad del administrador y operador de sistema.

- Consideraciones de las Auditorías de los sistemas de información
  - Controles de auditoria de los sistemas de información.

- Gestión de modificaciones con respaldo normativo
  - Registro del marco legal utilizado para realizar modificaciones sobre información procesada.
  - Registro de cambios periódicos que establezcan necesidades a ser cubiertas por desarrollos de módulos dentro del sistema.

## II. Alcance

El proceso de Auditoria 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 auditoria 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 exponen evidencias para cada caso expuesto en el anexo I.

En el **anexo III**, se facilitan guías de apoyo para mitigar alguna situación presentada la auditoria.

# CÓDIGO ADUANERO – LEY 2422/04

**Artículo 1°.- Función de la Aduana. Concepto.**
La Dirección Nacional de Aduanas es la Institución encargada de **aplicar la legislación aduanera**, recaudar los tributos a la importación y a la exportación, fiscalizar el tráfico de mercaderías por las fronteras y aeropuertos del país, ejercer sus atribuciones en zona primaria y realizar las tareas de represión del contrabando en zona secundaria.

# ANEXO I

## 1 POLITICAS – RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACION.

### 1.1 Documentación y procedimientos de operaciones.

- Nivel de Cumplimiento: BAJO
- Nivel de Riesgo: ALTO
- Situación Actual

  a. No existe un compendio integrado de políticas de gestión correspondiente a TI (Tecnología de Información), la operatoria actual se maneja bajo una metodología de "Buenas Prácticas".

- Recomendaciones

  a. Se deberían definir un conjunto de políticas para TI, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.
  b. Posterior a la confección de las políticas se deberá establecer la forma de institucionalizar las mismas, así como la asignación de los responsables de la actualización y control de la ejecución en las áreas pertinentes.
  c. En caso que el proceso de generación de las políticas se prolongue, se deberá documentar la metodología de buenas prácticas utilizada, y comunicar las mismas para conocimiento del personal del área, manejando esta opción como alternativa temporal.

### 1.2 Gestión de Cambios

- Nivel de Cumplimiento: MEDIO
- Nivel de Riesgo: MEDIO
- Situación Actual

  a. Dentro de la gestión de cambios no existen controles, sí registros y expedientes que sirven de respaldo pero no un control específico sobre lo realizado.

- Recomendaciones

a. Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.
b. Para la realización de los controles se debe establecer un proceso donde se determine el circuito desde la presentación de la solicitud, las modificaciones realizadas, las personas que realizaron el control de calidad y dieron su visto bueno al término de las pruebas hasta el momento de la publicación de la versión modificada en los servidores de producción.

## 1.3 Gestión de Capacidades

- Nivel de Cumplimiento: BAJO
- Nivel de Riesgo: MEDIO
- Situación Actual

a. Los recursos son monitoreados pero los resultados no son controlados, el proceso de afinación está supeditado a una situación que exija la actualización de las capacidades.
b. No se tiene respaldo documental de las proyecciones de los futuros requisitos de capacidad para asegurar la performance del SIS.
c. La mayoría de los recursos existentes, son suficientes para la necesidad actual.

- Recomendaciones

a. El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
b. Se debe evaluar todo recurso tanto de hardware como software que irá decayendo más rápido y proyectar las soluciones a corto / mediano plazo.

## 1.4 Separación de entornos de desarrollo, prueba y producción

- Nivel de Cumplimiento: ALTO
- Nivel de Riesgo: BAJO
- Situación Actual

a. Los entornos de desarrollo, prueba y producción están bien separados.

- Recomendaciones

a. Se recomienda la realización por medio de un cronograma de la actualización de los ambientes de prueba y desarrollo en base al de producción, para que de esta manera se minimice las posibles inconsistencias existentes por cambios que se van realizando. Esto debe incluir todos los objetos de la base de datos no solamente las tablas.

## 2 REGISTRO DE ACTIVIDAD Y SUPERVISION

### 2.1 Registro de gestión de eventos de actividad

- Nivel de Cumplimiento: MEDIO
- Nivel de Riesgo: MEDIO
- Situación Actual
    a. Se registran (logs) de eventos de actividades, pero no se realizan controles o revisiones sobre los mismos.
- Recomendaciones
    a. Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.
    b. Se debe asignar un responsable para la realización de estos controles.

### 2.2 Protección de los registros de información

- Nivel de Cumplimiento: MEDIO
- Nivel de Riesgo: MEDIO
- Situación Actual
    a. La información de los registros (logs) se generan y guardan en el proceso de backup, los mismos no se manejan de una manera directa, en caso de una situación se deberá recurrir a la búsqueda de los mismos en los servidores de respaldo.
- Recomendaciones
    a. Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidos contra la adulteración y el acceso no autorizado.
    b. Se debe crear un ambiente especifico o esquema donde se guarde la información de los registros (logs), el mismo debe ser accedido solamente por un usuario y el mismo debe estar bajo un esquema de control de registros de actividad, es decir no debe realizar otra operación que no sea la de consulta y se debe alertar en caso contrario.

### 2.3 Registros de actividad del administrador y operador de sistema

- Nivel de Cumplimiento: BAJO
- Nivel de Riesgo: MEDIO
- Situación Actual

- Recomendaciones

  a. Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.
  b. Así también se deben poder realizar seguimiento a operaciones realizadas por cualquier usuario, por ejemplo el usuario de consulta de los registros de auditoria.

# 3 CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACION

## 3.1 Controles de auditoría de los sistemas de información

- Nivel de Cumplimiento: MEDIO
- Nivel de Riesgo: MEDIO
- Situación Actual

  a. Dentro de la operatoria de la Administración SOFIA no se cuenta con un plan de trabajo a ser seguido para la realización de las Auditorias Internas y Externas correspondiente, permitiendo de esta manera organizar los tiempos y disponibilidad de las personas que se verán afectadas por esta tarea.
  b. No obstante se realizan las tareas de Auditoria bajo una coordinación con los Jefes de cada área, asignando el personal que estará disponible para poder recabar las evidencias solicitadas.

- Recomendaciones

  a. Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.

# 4 GESTION DE MODIFICACIONES CON RESPALDO NORMATIVO

## 4.1 Registro del marco legal utilizado en modificaciones que puedan establecer necesidades a ser cubiertas por desarrollos de módulos dentro del sistema.

- Nivel de Cumplimiento: MEDIO
- Nivel de Riesgo: ALTO
- Situación Actual

  a. En la actualidad se presentan solicitudes de modificación sobre información, registrada y procesada, dentro del sistema. Los motivos son diversos, pero sea cual fuese el caso, son cambios que se realizan por fuera del sistema y no siempre bajo un procedimiento que pueda delimitar la totalidad de modificaciones que se realizan para cumplir con el pedido; se facilita un cuadro que refleja algunas de las modificaciones más frecuentes. **Anexo II – Punto 1**

b. En cuanto a la existencia del procedimientos para realizar estos cambios, no se encontró nada que lo respalde; estos pedidos de modificación siguen unos pasos diferentes antes de que se llegue a la ejecución del mismo, durante estos pasos se va creando un expediente con toda la información de la tarea, entre los datos generales están las firmas de las autoridades competentes y el pedido del interesado.

c. En algunos de los expedientes a los cuales se tuvo acceso no hacen referencia a la normativa o procedimiento que ampare el pedido, simplemente solicitan un cambio y suelen dejar a criterios de los técnicos del SIS la factibilidad de la corrección.

d. Antes o después de la ejecución del pedido de modificación no se realiza ningún análisis de impacto, es decir, al no prever en qué puede afectar a otros datos o procesos la modificación de una información ya registrada, pueden generarse inconsistencias.

- Recomendaciones

a. Toda modificación a ser realizada sobre información ya procesada dentro de un sistema debe ser manejada como excepciones y deben de estar amparadas por alguna normativa, también las mismas deben tener un procedimiento definido con los pasos o circuitos a seguir, de esta manera se podrá realizar la trazabilidad en caso que se necesite hacer el seguimiento a una operación.

b. Cuando se realiza una modificación, el área que recibe el pedido debe corroborar que el documento esté conformado por las firmas de las autoridades competentes y los interesados, también que se referencie a las normativas o procedimientos que avale la operación solicitada para así estar amparado bajo la legislación vigente.

c. Para cada modificación que se realice en el sistema se debe anteponer un análisis del impacto y siempre tener un registro de lo realizado, tanto en papel como en forma digital.

Sin otro particular, me despido de usted atentamente.

Lic. Roberto Molinas
Auditor Informático – AGA

## ANEXO II (Evidencias)

**Punto 1**

| FRECUENCIA | TIPO | PROCESO | PROPUESTA |
|---|---|---|---|
| MUY FRECUENTE | HABILITACION TEMPORAL DESPACHANTE | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | DTO. DE REGISTRO |
| MUY FRECUENTE | HABILITACION TEMPORAL IMPORTADOR | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | DTO. DE REGISTRO |
| MUY FRECUENTE | HABILITACION TEMPORAL IMPORTADOR CASUAL | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | DTO. DE REGISTRO |
| MUY FRECUENTE | PRORROGA 10A3 | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS – APOYO | DIRECCION DE PROCEDIMIENTOS ADUANEROS |
| MUY FRECUENTE | CORRECCION DE CUMPLIDO DE EMBARQUE | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | ADMINISTRACIONES |
| FRECUENTE | REVERSA DE VISTURIA Y/O VALORACION | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | JEFE VISTURIA - ADMNISTRACIONES |
| FRECUENTE | CAMBIO DE DESTINO – INTERVENCION | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS – APOYO – SERCRETARIA – ADMINISTRACION – ADMINISTRACION DE ADUANA | DIRECCION DE PROCEDIMIENTOS ADUANEROS |
| FRECUENTE | DESBLOQUEO IC03 | ATENCION AL USUARIO – BASE DE DATOS | DIRECCION DE PROCEDIMIENTOS ADUANEROS |
| FRECUENTE | CAMBIO DE DESPACHANTE - LMAN | SECRETARIA – ADMINISTRACION – APOYO – BASE DE DATOS | DESPACHANTES |

Ejemplos de Intervenciones sin manifiesto/despacho asociado correspondiente al período (01/01/2016) al (21/06/2016).

| INTERVENCION | FECHA OPERACION | MANI | DESPACHO | ESTADO |
|---|---|---|---|---|
| 16UY0003672K | 22/2/2016 14:16 | | | REG |
| 16UY0003689S | 22/2/2016 14:16 | | | REG |
| 16UY0003690K | 22/2/2016 14:16 | | | REG |
| 16UY0002035C | 1/2/2016 17:52 | | | REG |
| 16UY0003807X | 22/2/2016 14:16 | | | REG |
| 16UY0003808J | 22/2/2016 14:16 | | | REG |
| 16UY0003809K | 22/2/2016 14:16 | | | REG |
| 16AR0000419C | 4/2/2016 11:40 | | | REG |
| 16UY0002947Y | 16/2/2016 11:06 | | | REG |
| 16CL0001126T | 19/2/2016 19:33 | | | REG |
| 16CL0001124P | 20/2/2016 11:10 | | | REG |
| 16CL0001125Z | 20/2/2016 11:10 | | | REG |
| 16CL0001126R | 20/2/2016 11:10 | | | REG |
| 16CL0001127S | 20/2/2016 11:10 | | | REG |

| | | | | |
|---|---|---|---|---|
| 16UY0003694Y | 22/2/2016 17:25 | | | REG |
| 16UY0003695P | 22/2/2016 17:25 | | | REG |
| 16UY0003700C | 22/2/2016 17:25 | | | REG |
| 16UY0003372H | 17/2/2016 16:09 | | | REG |
| 16UY0003373X | 17/2/2016 16:09 | | | REG |
| 16UY0003374J | 17/2/2016 16:10 | | | REG |
| 16UY0003375K | 17/2/2016 16:10 | | | REG |
| 16UY0003376L | 17/2/2016 16:10 | | | REG |
| 16UY0003377M | 17/2/2016 16:10 | | | REG |
| 16UY0003378N | 17/2/2016 16:10 | | | REG |
| 16UY0002952K | 19/2/2016 15:38 | | | REG |
| 16AR0000561A | 12/2/2016 15:11 | | | REG |
| 16AR0000671C | 22/2/2016 12:12 | | | REG |
| 16AR0000672D | 22/2/2016 12:15 | | | REG |
| 16AR0000673E | 22/2/2016 12:16 | | | REG |
| 16AR0000674F | 22/2/2016 12:18 | | | REG |
| 16AR0000675G | 22/2/2016 12:19 | | | REG |
| 16AR0000676H | 22/2/2016 12:20 | | | REG |
| 16AR0000677X | 22/2/2016 12:21 | | | REG |
| 16UY0003691L | 22/2/2016 15:45 | | | REG |
| 16UY0003692M | 22/2/2016 15:45 | | | REG |
| 16UY0003693N | 22/2/2016 15:45 | | | REG |
| 16UY0003487Y | 18/2/2016 17:27 | | | REG |
| 16UY0003488P | 18/2/2016 17:27 | | | REG |
| 16UY0003489Z | 18/2/2016 17:27 | | | REG |
| 16UY0003491J | 18/2/2016 17:27 | | | REG |
| 16UY0003492K | 18/2/2016 17:27 | | | REG |
| 16UY0003493L | 18/2/2016 17:27 | | | REG |
| 16UY0003494M | 18/2/2016 17:27 | | | REG |
| 16CL0001121M | 19/2/2016 17:21 | | | REG |
| 16UY0002252D | 3/2/2016 16:06 | | | REG |
| 16CL0000962B | 17/2/2016 10:16 | | | REG |
| 16CL0000967G | 17/2/2016 10:53 | | | REG |
| 16UY0003395M | 17/2/2016 16:11 | | | REG |
| 16UY0003396N | 17/2/2016 16:11 | | | REG |
| 16UY0003397Y | 17/2/2016 16:11 | | | REG |
| 16UY0003398P | 17/2/2016 16:11 | | | REG |
| 16UY0003400W | 17/2/2016 16:11 | | | REG |
| 16UY0003401A | 17/2/2016 16:11 | | | REG |
| 16UY0003500A | 22/2/2016 15:21 | | | REG |
| 16UY0003501B | 22/2/2016 15:22 | | | REG |
| 16UY0003502C | 22/2/2016 15:22 | | | REG |
| 16UY0003503D | 22/2/2016 15:22 | | | REG |

| | | | | |
|---|---|---|---|---|
| 16UY0003504E | 22/2/2016 15:23 | | | REG |
| 16UY0003544X | 22/2/2016 15:35 | | | REG |
| 16UY0003545J | 22/2/2016 15:36 | | | REG |
| 16TRA000022F | 28/1/2016 14:49 | | | REG |
| 16UY0003546K | 22/2/2016 15:36 | | | REG |
| 16UY0003547L | 22/2/2016 15:36 | | | REG |
| 16UY0003548M | 22/2/2016 15:36 | | | REG |
| 16UY0003549N | 22/2/2016 15:37 | | | REG |
| 16UY0003550F | 22/2/2016 15:37 | | | REG |
| 16UY0003551G | 22/2/2016 15:37 | | | REG |
| 16UY0003552H | 22/2/2016 15:37 | | | REG |
| 16UY0003553X | 22/2/2016 15:38 | | | REG |
| 16UY0003554J | 22/2/2016 15:38 | | | REG |
| 16UY0003555K | 22/2/2016 15:38 | | | REG |
| 16UY0003556L | 22/2/2016 15:39 | | | REG |
| 16UY0003557M | 22/2/2016 15:39 | | | REG |
| 16UY0003558N | 22/2/2016 15:39 | | | REG |
| 16UY0003559Y | 22/2/2016 15:39 | | | REG |
| 16UY0003560G | 22/2/2016 15:40 | | | REG |
| 16UY0003561H | 22/2/2016 15:40 | | | REG |
| 16UY0003562X | 22/2/2016 15:41 | | | REG |
| 16UY0003563J | 22/2/2016 15:41 | | | REG |
| 16CL0000896H | 12/2/2016 14:50 | | | REG |
| 16CL0000176V | 15/1/2016 13:47 | | | REG |
| 16UY0002872L | 12/2/2016 15:42 | | | REG |
| 16CL0000986H | 18/2/2016 09:59 | | | REG |
| 16UY0003443G | 18/2/2016 10:08 | | | REG |
| 16UY0003446J | 18/2/2016 10:08 | | | REG |
| 16UY0003448L | 18/2/2016 10:10 | | | REG |
| 16CL0000985G | 18/2/2016 10:12 | | | REG |
| 16CL0000992E | 18/2/2016 10:12 | | | REG |
| 16CL0000991D | 18/2/2016 10:12 | | | REG |
| 16UY0003449M | 18/2/2016 10:17 | | | REG |
| 16UY0003451F | 18/2/2016 10:17 | | | REG |
| 16UY0003452G | 18/2/2016 10:17 | | | REG |
| 16TRA000039N | 22/2/2016 13:42 | | | REG |
| 16CL0001052P | 18/2/2016 16:29 | | | REG |

Ejemplos de Liquidaciones bajo el **concepto 500** correspondiente al periodo (01/01/2016) al (21/06/2016).

| NRO LIQUIDACION | DESPACHO | FECHA EMISION | ESTADO | CONCEPTO | TIPO PAGO | MONTO |
|---|---|---|---|---|---|---|
| 16017INTE002830J | 16017IC13000004F | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16017INTE002833M | 16017IC04001620K | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16024INTE000916K | 16024IC04000618Y | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16017INTE002842M | 16017IC04001621L | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16017INTE002844Y | 16017IC04001622M | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16024INTE000917L | 16024IC04000619P | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16019INTE001674Z | 16019IC04000770R | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16019INTE001676S | 16019IC04000771S | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16019INTE001677T | 16019IC04000772T | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16019INTE001678U | 16019IC04000773U | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16017INTE002959V | 16017IC04001682S | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16024INTE000927M | 16024IC04000628P | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16024INTE000929Y | 16024IC04000629Z | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16024INTE000930G | 16024IC04000630X | 3/2/2016 | PAG | 500 | P | 293,597 |
| 16017INTE004667T | 16017IC04002537S | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16030INTE002289M | 16030IC04001631H | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16017INTE004668U | 16017IM04000082V | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16024INTE001345H | 16024IC04000908Z | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16030INTE002291F | 16030IC04001633J | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16032INTE000842H | 16032IC04000402E | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16031INTE000663H | 16031IC04000355K | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16019INTE002560L | 16019IC04001088U | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16017INTE004669V | 16017IC04002538T | 19/2/2016 | PAG | 500 | P | 290,091 |
| 16027INTE000301B | 16027IC04000226M | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002634L | 16017IC04001498A | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002635M | 16017IC04001499B | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002636N | 16017IC04001500H | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16024INTE000865N | 16024IC04000573Y | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16019INTE001556P | 16019IC04000706Z | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE004250H | 16017IC04002316N | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16024INTE001247X | 16024IC04000839T | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16017INTE004251X | 16017IC04002317Y | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16024INTE001248J | 16024IC04000840L | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16015INTE001673L | 16015IC04001245L | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16019INTE002363M | 16019IC04001008M | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16024INTE001250C | 16024IC04000842N | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16017INTE004252J | 16017IC04002318P | 16/2/2016 | PAG | 500 | P | 289,669 |
| 16029INTE000811J | 16029IC04000530M | 16/2/2016 | PAG | 500 | P | 289,669 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 16017INTE004464Y | 16017IC04002428R | 18/2/2016 | PAG | 500 | P | 290,022 |
| 16017INTE004465P | 16017IC04002429S | 18/2/2016 | PAG | 500 | P | 290,022 |
| 16019INTE002448Z | 16019IC04001046Y | 18/2/2016 | PAG | 500 | P | 290,022 |
| 16023INTE001041W | 16023IC04000178Y | 18/2/2016 | PAG | 500 | P | 290,022 |
| 16017INTE004469T | 16017IC04002433N | 18/2/2016 | PAG | 500 | P | 290,022 |
| 16031INTE000423B | 16031IC04000220B | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16024INTE000875Y | 16024IC04000583P | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16031INTE000425D | 16031IC04000222D | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16025INTE000929P | 16025IC04000088Z | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16004INTE000244C | 16004IC04000062F | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002690N | 16017IC04001544P | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002691Y | 16017IC04001545Z | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16017INTE002601F | 16017IC04001483R | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16031INTE000417E | 16031IC04000217H | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16027INTE000304E | 16027IC04000229P | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16027INTE000331E | 16027IC04000240X | 1/2/2016 | PAG | 500 | P | 296,627 |
| 16027INTE000413F | 16027IC04000302H | 8/2/2016 | PAG | 500 | P | 293,307 |
| 16024INTE001037F | 16024IC04000692Z | 8/2/2016 | PAG | 500 | P | 293,307 |
| 16024INTE001038G | 16024IM04000025Z | 8/2/2016 | PAG | 500 | P | 293,307 |
| 16024INTE001039H | 16024IC04000693R | 8/2/2016 | PAG | 500 | P | 293,307 |
| 16017INTE000394M | 16017IC04000246N | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000395N | 16017IC04000247Y | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000396Y | 16017IC04000248P | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16027INTE000065X | 16027IC04000059Z | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000399R | 16017IC04000249Z | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000401B | 16017IC04000250X | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16024INTE000140W | 16024IC04000088P | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16021INTE000033U | 16021ZF01000016U | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000402C | 16017IC04000251J | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000706J | 16017IC04000419P | 11/1/2016 | PAG | 500 | P | 293,862 |
| 16017INTE000734K | 16017IC04000440J | 11/1/2016 | PAG | 500 | P | 293,862 |
| 16017INTE001220B | 16017IC04000719S | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16019INTE000952Y | 16019IC04000358T | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16017INTE001221C | 16017IC04000720K | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16030INTE000529H | 16030IC04000384L | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16019INTE000953P | 16019IC04000359U | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16019INTE000954Z | 16019IC04000360M | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16030INTE000530W | 16030IC04000385M | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16017INTE001222D | 16017IC04000721L | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16019INTE000955R | 16019IC04000361N | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16030INTE000531A | 16030IC04000386N | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16017INTE001223E | 16017IC04000722M | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16032INTE000197K | 16032IC04000114E | 15/1/2016 | PAG | 500 | P | 295,608 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 16017INTE000091G | 16017IC04000062J | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16032INTE000018C | 16032IC04000017G | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16017INTE000102W | 16017IC04000072K | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16017INTE000140B | 16017IC04000098S | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16017INTE000141C | 16017IC04000099T | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16017INTE000147X | 16017IC04000104G | 5/1/2016 | PAG | 500 | P | 291,737 |
| 16017INTE004365Y | 16017IC04002373Z | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16017INTE004366P | 16017IT02000053B | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16017INTE004367Z | 16017IC04002374R | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16003INTE001801B | 16003IC04001063G | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16003INTE001802C | 16003IC04001064H | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16017INTE004369S | 16017IC04002375S | 17/2/2016 | PAG | 500 | P | 290,106 |
| 16027INTE000553K | 16027IC04000382P | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16017INTE004168P | 16017IC04002265Z | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16019INTE002330G | 16019IC04000993B | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16030INTE002038E | 16030IC04001460H | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16017INTE004169Z | 16017IC04002266R | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16030INTE002045C | 16030IC04001463K | 15/2/2016 | PAG | 500 | P | 290,851 |
| 16017INTE000370G | 16017IC04000233J | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000371H | 16017IC04000234K | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000373J | 16017IC04000235L | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000205F | 16019IC04000121H | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000374K | 16017IC04000236M | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16023INTE000076G | 16023IC04000016F | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16005INTE000645X | 16005IC04000248M | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16032INTE000065E | 16032IC04000050D | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000252H | 16019IC04000151K | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16005INTE000649M | 16005IC04000249N | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000471X | 16017IC04000290M | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000253X | 16019IC04000152L | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000254J | 16019IC04000153M | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16032INTE000066F | 16032IC04000051E | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000255K | 16019IC04000154N | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16017INTE000473K | 16017IC04000291N | 7/1/2016 | PAG | 500 | P | 293,023 |
| 16019INTE000258N | 16019IC04000155Y | 7/1/2016 | PAG | 500 | P | 295,608 |
| 16007INTE000160C | 16007IC04000045J | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16024INTE000401W | 16024IC04000269Z | 15/1/2016 | PAG | 500 | P | 295,608 |
| 16030INTE000522A | 16030IC04000377N | 15/1/2016 | PAG | 500 | P | 295,608 |

# ANEXO III (Guías)

## Guía para establecer Políticas de Seguridad de la Información (PSI)

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar.

Es importante que al momento de formular las políticas de seguridad de la información, se consideren por lo menos los siguientes aspectos:

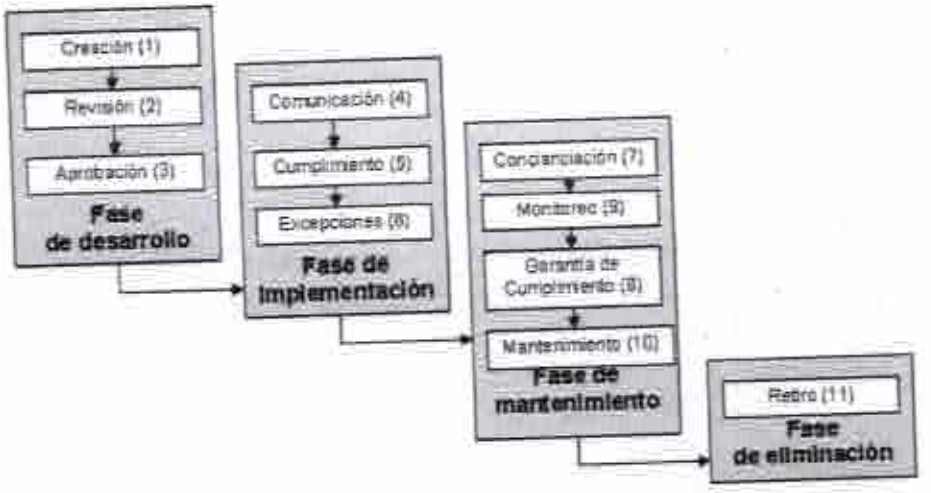
- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.
- Monitorear periódicamente los procedimientos y operaciones de la institución, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Para aclarar los términos utilizados se definen los siguientes:.

| | |
|---|---|
| POLÍTICA | Declaración general de principios que presenta la posición de la institución para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, |

| | |
|---|---|
| | procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por las directivas de la universidad, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción. |
| ESTÁNDAR | Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas. |
| MEJOR PRÁCTICA | Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización. |
| GUÍA | Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo. |
| PROCEDIMIENTO | Los procedimientos definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema. Los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican. |

ETAPAS EN EL DESARROLLO DE UNA POLÍTICA




## Aspectos a incluir en una política de Seguridad de la Información

- **Alcance y ámbito de la Política de Seguridad**: En este punto se debe detallar si la política es global, para toda la empresa, o si está delimitada para determinados departamentos o personas.

- **Responsabilidades y Organización de la Seguridad de la Información:** Se establecerá una estructura de responsables para la toma de decisiones respecto a inversiones, seguimiento y aseguramiento del cumplimiento de lo recogido en las políticas. Así mismo, puede establecerse la composición de un Comité para la toma de decisiones conjuntas en materia de seguridad.

- **Control de la información**: Se indicarán las pautas para asegurar el buen uso de la información. Una buena práctica puede ser establecer una guía de clasificación de la información en función de su contenido y/o grado de confidencialidad. A cada nivel (por ejemplo: información de uso interno, confidencial, reservada), se le dotarán de diferentes medidas de seguridad en cada una de sus fases de tratamiento (creación, distribución, eliminación).

- **Seguridad del personal:** Se especificarán las medidas de seguridad a tomar en relación al personal de la organización desde su incorporación en la que deberían firmarse acuerdos y cláusulas de confidencialidad, uso de los sistemas, etc., pasando por su permanencia en la empresa, en la que deberá establecerse un programa de formación y concienciación en Seguridad de la Información hasta la finalización de la relación laboral donde se detallarán

las medidas para asegurar la devolución del equipamiento(móviles, portátiles, etc.) que hayan sido cedidos al empleado para su desarrollo de actividades en la empresa y la eliminación de autorizaciones de acceso.

- **Seguridad física:** Hablar de seguridad informática no es solo hablar de un hacker o de un PC que ha perdido los datos, debemos de tomar medidas para asegurar que, físicamente, nuestros equipos de procesamiento de datos están protegidos contra fuego, inundación o robo.

- **Seguridad en las comunicaciones:** Se trata de un apartado meramente técnico y orientado al equipamiento informático, en el deberá recogerse los mecanismos para el control de código malicioso (por ejemplo, los PC's deberán contar con un antivirus actualizado), la estrategia a seguir para la gestión de copias de seguridad o el uso que los empleados pueden hacer de Internet o del correo electrónico corporativo.

- **Control de los accesos a los sistemas de información**: Este punto debiera especificar cómo debe ser la política de asignación de privilegios y gestión de usuarios orientado a evitar el acceso no autorizado a los sistemas y activos de información. No todos los empleados deben tener acceso a toda la información y, este es el punto, en el que debe especificarse cuál es el principio en el que se basará la asignación de privilegios. Un ejemplo es establecer los mismos en base al principio de "necesidad de conocer", es decir, nadie debe tener acceso a aquello que no deba conocer para ejecutar su actividad.

- **Mantenimiento de las aplicaciones**: Deberá recoger cómo será la estrategia para mantener las aplicaciones, como se asegurará que los PC's son actualizados, con qué periodicidad, etc.

- **Continuidad del negocio:** ¿Ha pensado alguna vez en qué pasaría si su oficina saliese ardiendo? A menudo, no somos conscientes de las amenazas que nos rodean hasta que nos damos cuenta...y desgraciadamente, suele ser demasiado tarde. En la política de seguridad deben recogerse qué medidas deben tomarse para asegurar que un "accidente" no paraliza nuestro negocio.