POLÍTICA DE SEGURIDAD DE LA INFORMACION Y DEL SISTEMA INFORMATICO

1.- DEFINICIÓN

La presente política de seguridad de la información de Asesoría y Gestión en Aduanas S.A., define los objetivos, alcances y principios esenciales para la administración, custodia y el uso de activos de información, velando por su disponibilidad, confidencialidad e integridad, acorde a los requisitos de seguridad del modelo BASC, OEA e ISO 27001.

2.- OBJETIVO DE LA POLÍTICA

La política de seguridad de la información y del Sistema Informático de Asesoría y Gestión en Aduanas S.A., tiene los siguientes objetivos:

- Resguardar los activos de información de la empresa Asesoría y Gestión en Aduanas S.A. frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, considerándolos resultados de la evaluación y tratamiento de riesgos.
- Implementar medidas especiales de seguridad, teniendo como base esta política.

3.- ALCANCE O ÁMBITO DE APLICACIÓN

- Esta política es aplicable y extensiva a todo el personal, independiente de su modalidad de contratación; y a terceros, naturales o jurídicos que presten servicios en forma permanente o temporal en la empresa Asesoría y Gestión en Aduanas S.A.
- Consecuente a lo anterior, los terceros deberán conocer y acatar la presente política y las que de ésta se desprendan, lo que quedará expresamente consignado en los respectivos contratos o acuerdos de servicio.

4.- ROLES Y RESPONSABILIDADES

Asesoría y Gestión en Aduanas S.A. mantendrá una adecuada organización relacionada con la seguridad de la información y la seguridad informática, el mismo que definirá un encargado de la seguridad de la información y la seguridad informática.

- El comité de seguridad de la información y la seguridad informática deberá proponer las medidas de seguridad destinadas a proteger y preservar los activos de la información de la institución y velar por el cumplimiento de las políticas de ciberseguridad y seguridad de la información.
- El encargado de la seguridad de la información y la seguridad informática deberá coordinar la implantación y efectiva aplicación de las medidas de seguridad que se definan.

Rol	Responsabilidades	Cargo
Comité de Seguridad de la información y la Seguridad informática	- Proponer las políticas en materia de seguridad de la información - Prevenir pérdidas patrimoniales o que comprometan los recursos - Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y estable de recursos de información que sea consciente con las metas y objetivos de la empresa. - Proveer dirección y experiencia para asegurar que la información se encuentre protegida apropiadamente, sobre los supuestos de la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos y físicos que lo soportan. - Proponer estrategias para la divulgación de la política a todas las partes interesadas. - Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. - Evaluación de los procesos de la seguridad de la información y del sistema informático - Evaluación del encargado de la seguridad de la información y del sistema informático - Coordinar la Elaboración del Programa de Auditoria	-Coordinador OEA - Coordinador de Exportaciones e Importaciones. -Encargada de Recursos Humanos -Gerente de Administración y Finanzas -Encargada de Seguridad
	- Administrar la red, sistemas operativos, aplicaciones y base de datos propios	-Encargado de Sistemas

Encargado de la seguridad de la información y la seguridad informática	- Administrar la página web - Procurar que la integridad, autentificación, control de acceso, implantación y operación de los sistemas de información - Procurar la confidencialidad, integridad y disponibilidad de la información almacenada en los sistemas de información, así como su salvaguarda mediante copias de seguridad periódicas. - Conceder a los usuarios acceso únicamente a los datos y recursos a los que estén autorizados y precisen para el desarrollo de su trabajo. - Levantar el inventario de activos tecnológicos de la información - Generar el Plan de Mantenimiento, operación, monitoreo y mejora continua del Modelo de Seguridad de la Información - Gestionar el análisis, definición del Alcance, implementación, mantenimiento y mejora continua de las normas de seguridad de la información y del Sistema Informático. - Aplicar conocimientos, habilidades, herramientas y técnicas a las actividades propias del negocio de manera que cumpla o exceda las necesidades y expectativas de los interesados del mismo. - Minimizar los riesgos de Seguridad para la continuidad del negocio	

5.- PARTES INTERESADAS, NECESIDADES Y EXPECTATIVAS

Asesoría y Gestión en Aduanas S.A. ha determinado las partes interesadas de acuerdo al Anexo 1 de Matriz de Partes interesadas:

- ✓ Accionistas
- ✓ Colaboradores
- ✓ Clientes
- ✓ Proveedores
- ✓ Gobierno

La información que requiera Asesoría y Gestión en Aduanas S.A. para satisfacer sus necesidades y expectativas de las partes interesadas antes mencionadas en el ámbito de sus funciones, encomendadas por el grupo de accionistas, deberá estar protegida en sus dimensiones de disponibilidad, integridad y confidencialidad.

6.- INVENTARIO, CLASIFICACION Y CONTROL DE ACTIVOS

6.1. Inventario de activos.

El Comité de Seguridad de la información es el encargado de identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación, asimismo deberá de actualizarlo ante cualquier modificación y revisarlo con periodicidad anual

6.2. Clasificación de la información.

Para clasificar un Activo de Información, se evaluarán las tres características de la información: confidencialidad, integridad y disponibilidad.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACION PUBLICA RESERVADA	ALTA	ALTA
INFORMACION PUBLICA CLASIFICADA	MEDIA	MEDIA
INFORMACION PUBLICA	BAJA	BAJA
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

ALTA	Activos de información en los cuales la clasificación de la información tiene 2 o todas las propiedades de seguridad (confidencialidad, integridad y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad y disponibilidad) o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja

Asesoría y Gestión en Aduanas S.A. ha determinado el inventario y clasificación de criticidad de los activos de Seguridad Informática acuerdo al Anexo Nro. 2.

6.3 Rotulado de la Información.

El encargado de Seguridad Informática definirá el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los activos de información electrónicos.

8.- LINEAMIENTOS DE LA POLITICA

En Asesoría y Gestión en Aduanas S.A. es primordial la importancia de la Seguridad de la Información y del Sistema Informático, por lo que se compromete a gestionar la Seguridad de la Información y del Sistema Informático como un proceso continuo, a través de la implementación de normas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información

Políticas Generales

- Protegemos la infraestructura de las tecnologías de la información con seguridad perimétrica a través de un Firewall Fortinet.
- Se reconoce la información como activo, valioso y fundamental para la empresa, que debe ser administrado y protegido.

- Se define como seguridad de la información a toda acción que busque proteger la integridad, confidencialidad y disponibilidad de los activos de la información.
- Reconocer el compromiso de toda la organización, de cautelar y velar por la confidencialidad y reserva de la información que la instituciones, los agentes de comercio exterior, las empresas importadoras / exportadoras le han proporcionado u obtenido en el ejercicio de sus funciones; y también, a suministrar la disponibilidad de acceso a esta información.
- La seguridad de la información asociado a su manejo, es responsabilidad de todos los colaborares, independiente del cargo o funciones que desempeñen; y de terceros.

- Las Normas y políticas sobre Seguridad de la información, serán debidamente controladas y auditadas en su cumplimiento por el comité de Seguridad de la información y la Seguridad informática.
- El incumplimiento de las obligaciones de esta Política, procedimiento u otros documentos de seguridad de la información y del Sistema informático serán sancionadas bajo el Reglamento de la empresa y podrá poner término a su contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades penales y legales que se deriven tales infracciones.
- En los casos donde exista una necesidad justificable de realizar acciones excepcionales, que estén en conflicto con las medidas establecidas en esta política, deberán ser evaluadas por el comité de Seguridad de la información y la Seguridad informática.
- La política de seguridad de la información y del Sistema Informático serán publicadas en la página web, así mismo se sensibilizará al interior de la empresa a través de charlas, talleres, boletines y/o publicaciones la importancia de la Seguridad de la información.

Políticas Específicas y de Ciberseguridad.

- Todos los equipos que se conecten a la red de datos de la organización deben ser previamente autorizados, autentificados mediante usuario y contraseña y bajo un perfil de acceso que determine la información a la que puede acceder.
- La información contenida en los sistemas es propiedad confidencial de la organización, por lo cual los usuarios no deben utilizar los equipos y sistemas para contener información personal.
- Mantener el respeto a la propiedad intelectual y derechos de autor en el uso de programas y licencias dentro de la organización.
- No ingresar a páginas webs no autorizadas, sitios desconocidos o no confiables.
- Los usuarios no deben intentar violentar los sistemas de seguridad y de control de accesos.

- La pérdida ó robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al encargado de Sistemas.
- No aceptar la instalación automática de software a pesar de estar restringido esta acción.
- No descargar archivos ejecutables.
- Comprometerse en no interferir en el uso adecuado de los recursos de la Red: o NO instalar impresoras de red automáticamente o NO crear unidades lógicas adicionales en la red.
- El protector de pantalla y el fondo del escritorio es el mismo para todos, no debe cambiarse.

- Al momento de ausentarse bloquear sus equipos (Inicio de Windows + L = Bloqueo de Equipo). En caso no se bloquee el equipo, este después de 5 minutos automáticamente se bloqueará.
- No compartir sus contraseñas. El hacerlo expone al usuario a las consecuencias por las acciones que los otros realicen con esa contraseña.
- El encargado de sistemas cambia periódicamente las contraseñas (Cada 06 meses). y cada vez que la contraseña haya sido vulnerada o se presuma de alguna actividad sospechosa.
- No debe guardar su contraseña en una forma legible, en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe reportarla inmediatamente al encargado de sistemas para su cambio. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas.
- Guardar una copia de seguridad de la información sensible en la Nube asociada al correo Office 365 con el objeto de salvaguardar la información.

9.- PERIODO DE VIGENCIA

Esta política tiene una vigencia indeterminada, sin embargo, se efectuará una revisión del contenido de este documento anualmente por el comité de seguridad de la información y seguridad informática, o cuando deban atenderse necesidades de cambios significativos, para garantizar su idoneidad, adecuación y efectividad; o cuando presenten cambios en el contexto interno o externo; o cuando se materialice un riesgo, o cuando sea presentado y sustentado como requerimiento expreso de cualquier de sus miembros del comité.

10.- EVALUACION DEL CUMPLIMIENTO

La evaluación de la aplicación de esta política, se realizará anualmente a través del formato de Evaluación del Cumplimiento TI….

NOTA: EL INCUMPLIMIENTO DE LAS POLITICAS MENCIONADAS CONLLEVARÁ A SANCIONES QUE DETERMINARÁ LA GERENCIA GENERAL.

ASESORIA Y GESTION EN ADUANAS S.A.
JULIO CÉSAR PALOMINO CAMINO
GERENTE GENERAL

Julio César Palomino Camino
Gerente General