ANEXO

Política de Seguridad de la Información de la Dirección Nacional de Aduanas

1 Introducción

La información es un activo esencial para las Organizaciones y adopta diversas formas: puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, estar impresa o escrita en papel, mostrada en video o hablada en conversación. Cualquiera que sea la forma que tome la información, o los medios por los que se comparta o almacene, la misma debe ser siempre protegida adecuadamente.

La Seguridad de la Información es la protección de la información contra una amplia gama de amenazas, para asegurar la continuidad de las operaciones, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de mejora.

La Seguridad de la Información se caracteriza como la preservación de:

a) su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información;
b) su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
c) su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

2 Objetivo

El propósito de esta política es el de proteger los activos de información de la D.N.A de todas las amenazas, ya sean externas o internas, intencionales o accidentales.

3 Ámbito de aplicación

Esta política es de aplicación a todos los individuos que utilizan los Recursos de Información de la D.N.A, independiente del cargo que desempeñen y de su situación contractual.

4 Política

La Dirección de la D.N.A reconoce la importancia de identificar y proteger los activos de información del Organismo. Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

Un Sistema de Gestión de Seguridad de la Información es un conjunto de controles, políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software, adecuados para lograr preservar la confidencialidad, integridad y disponibilidad de la información; minimizando los riesgos asociados. Estos controles deben ser establecidos, implementados, supervisados, revisados y mejorados cuando sea necesario, para asegurar que se cumplen los objetivos específicos de seguridad de la Organización.

La Dirección de la D.N.A. designará un Responsable de la Seguridad de la Información y conformará un Comité de Seguridad de la Información. Dicho Responsable se encargará

de la guía, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información, así como también liderará el mencionado Comité, que tendrá como cometido la definición de políticas, procesos y procedimientos vinculados a la Seguridad de la Información, que sean de aplicación transversal a toda la Organización.

La seguridad de la información que puede lograrse a través de medios técnicos es limitada, y debe apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deben instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información requiere la participación de todos los funcionarios de la D.N.A, así como también de las terceras partes que trabajan en la D.N.A o intervienen en la operativa aduanera.

Es política de la D.N.A:

a) Establecer objetivos anuales con relación a la Seguridad de la Información.
b) Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, y de acuerdo a su resultado implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.
c) Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración en relación a la importancia que posee para la D.N.A.
d) Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad.
e) Brindar concientización y formación en materia de seguridad de la información a todo el personal.
f) Contar con una política de gestión de incidentes de seguridad de la información de acuerdo a los lineamientos establecidos por el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy).
g) Establecer que todo el personal es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas, de acuerdo a los procedimientos correspondientes.
h) Establecer los medios necesarios para garantizar la continuidad de las operaciones del Organismo.

5 Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política regulada en el presente documento, la Dirección de la D.N.A podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

6 Referencias

- Política de Seguridad de la Información de A.G.E.S.I.C.
- Política de Seguridad de la Información del MEF (resolución MEF 2011-12)