

**OFICINA DEL PRESIDENTE EJECUTIVO*****ORDEN ADMINISTRATIVA***NÚMERO: OA-2011-17DISTRIBUCIÓN: “D”FECHA: 14 de diciembre de 2011**ASUNTO: POLÍTICA DE AVALÚO DE RIESGOS****PROPÓSITO:**

El propósito de esta política es garantizar que los riesgos de los sistemas de información de la Autoridad de Acueductos y Alcantarillados (AAA) sean identificados, analizados y mitigados, manteniéndolos en niveles aceptables y así contribuir con la responsabilidad de salvaguardar los recursos de la AAA.

EXPOSICIÓN DE MOTIVOS:

Esta política aplica a toda la información de los sistemas de la AAA, que incluye aplicaciones, servidores, redes y todos los procesos manejados en éstos sistemas.

También aplica a todos los departamentos y funciones que colecten, transmitan o manejen información en los sistemas de la AAA.

DEFINICIÓN DE TÉRMINO:

1. Evaluación del Riesgo – se define como el proceso general de evaluación y análisis de riesgo.
2. Mitigar Riesgo – se refiere a las acciones que deben tomarse para reducir la probabilidad de que un evento que perjudique la operación de la organización ocurra, o para minimizar el impacto. El riesgo nunca puede ser totalmente eliminado, pero puede mitigarse para disminuir su probabilidad y/o impacto.
3. Riesgo – es la probabilidad de que eventos o condiciones que puedan ocurrir y cuya aparición, si se llevara a cabo, tiene un impacto perjudicial o negativo en el logro de los objetivos de negocio de una organización.
4. Sistemas de Información – se refiere a programas, aplicaciones, dispositivos, bases de datos, redes de comunicación y archivos electrónicos.

RESPONSABILIDADES:

1. El Director Auxiliar de Seguridad Informática y/o personal designado por éste es responsable de:
 - a. Coordinar el desarrollo y mantenimiento de las políticas de avalúo de riesgos, procedimientos y normas para el Departamento de Sistemas de Información.
 - b. Ejecutar y gestionar diariamente el programa de administración de riesgos de la Autoridad para la seguridad y privacidad de la información.
 - c. Notificar al Director de Sistemas de Información las estrategias de evaluación de riesgos y proporcionar informes periódicos sobre los avances del programa.
2. Los Directores Auxiliares y Gerentes del Departamento de Sistemas de Información evaluarán los resultados de la evaluación de riesgos y presentarán al Director Auxiliar de Seguridad Informática los planes para mitigar los riesgos detectados.

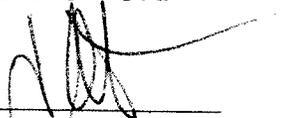
DETERMINACIÓN:

1. Los planes de mitigación de riesgos detallarán las acciones y estrategias necesarias a realizar, así como las fechas propuestas de implantación.
2. Las evaluaciones de riesgo se realizaran al menos una vez al año a todos los sistemas de información siguiendo las guías del Director Auxiliar de Seguridad Informática sobre el método de evaluación, formato, contenido y frecuencia.
3. El Director de Sistemas de información debe presentar un informe a la alta gerencia resumiendo los resultados de la evaluación de riesgos.

VIGENCIA:

Esta Orden Administrativa tiene vigencia inmediata.

APROBADO POR:



Ing. José F. Ortiz Vázquez
Presidente Ejecutivo

12/23/2011
Fecha de Aprobación