

**OFICINA DEL PRESIDENTE EJECUTIVO*****ORDEN ADMINISTRATIVA***NÚMERO: OA-2011-15DISTRIBUCIÓN: “D”FECHA: 16 de noviembre de 2011**ASUNTO: POLÍTICA DE MANEJO DE LA RED DE COMUNICACIONES****PROPÓSITO:**

El propósito de esta política es establecer una guía que garantice un adecuado manejo de la red de comunicaciones de la Autoridad de Acueductos y Alcantarillados (AAA).

EXPOSICIÓN DE MOTIVOS:

Esta política aplica a todo el personal responsable del manejo de la red de comunicaciones de la AAA.

DEFINICIÓN DE TERMINOS:

1. “Firewall” – parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo las comunicaciones autorizadas.
2. Red de comunicaciones – es una conexión de diferentes computadoras que pueden comunicarse e intercambiar información utilizando sus propios recursos o ajenos.

DETERMINACIÓN:

1. La red de comunicaciones de la Autoridad estará manejada por personal debidamente autorizado y capacitado de manera que se preserve su seguridad e integridad.
2. El diseño de la red de comunicaciones se realizará con el apoyo del personal necesario para una correcta definición de los requerimientos técnicos y funcionales de la red.

3. El diseño y la configuración de la red de comunicaciones deberá ofrecer un rendimiento adecuado y confiable que satisfaga las necesidades de la Autoridad.
4. La red de comunicaciones estará protegida por mecanismos de control, tales como: "firewalls", antivirus, sistemas monitoreo, entre otros.
5. El acceso a los recursos de la red deberá ser controlado mediante la utilización de mecanismos de control de acceso.
6. Los administradores de redes de comunicación serán responsables de analizar el tráfico de la red con el propósito de registrar estadísticas de utilización y niveles de servicio.
7. Los administradores de redes de comunicación serán responsables de seguir las prácticas de seguridad de información al implementar equipos de telecomunicación, tales como: enrutadores (*routers*), (*switches*), entre otros.
8. No se permitirá la instalación de herramientas para la captura de paquetes de información a menos que sean formalmente autorizadas y de total conocimiento por parte de los administradores de redes de comunicación.
9. No se permitirá la interconexión de redes externas sin la evaluación de sistemas de Información.
10. La interconexión de redes de terceros debe contemplar todas las medidas de seguridad para salvaguardar y minimizar el funcionamiento óptimo de la red.
11. La interconexión de VPNs con redes de terceros debe ser previamente autorizada por el Departamento de Sistemas luego de evaluar los riesgos de seguridad que pudiesen haber.
12. Toda interconexión con terceros debe tener la firma de un Non – "Disclosure Agreement" entre las partes.
13. Bajo ninguna circunstancia se permitirán conexiones directas con terceros sin mediar dispositivos de seguridad que permita salvaguardar y minimizar riesgos de seguridad.
14. Las redes internas de la Autoridad que no sean parte de la red administrativa se considerarán redes externas y deben seguir el mismo trato para minimizar los riesgos de seguridad y garantizar el funcionamiento de ambas redes.
15. Está totalmente prohibido la transmisión de "streaming" de video en la red administrativa de la Autoridad, excepto en aquellos casos autorizados por el Departamento de Sistemas y para ello se buscarán todas las medidas para que el tráfico no compita con las aplicaciones principales.

16. Está totalmente prohibido hacer "scanning" o "sniffing" de la red excepto en situaciones especiales autorizadas por el Departamento de Sistemas.
17. No se permitirá la conexión de dispositivos activos de comunicación ("routers", "routers" inalámbricos, "switches", etc.) sin la debida autorización del Departamento de Sistemas.

VIGENCIA:

Esta Orden Administrativa tiene vigencia inmediata.

APROBADO POR:



Ing. José F. Ortiz Vázquez
Presidente Ejecutivo

12/23/2011
Fecha de Aprobación