

**OFICINA DEL PRESIDENTE EJECUTIVO*****ORDEN ADMINISTRATIVA***NÚMERO: OA-2011-05DISTRIBUCIÓN: “D”FECHA: 13 de julio de 2011**ASUNTO: POLÍTICA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN****PROPÓSITO:**

El propósito de esta política es establecer las directrices y parámetros mínimos de seguridad para el manejo y administración de los sistemas de información, así como la seguridad física del Departamento de Sistemas de Información.

EXPOSICIÓN DE MOTIVOS:

Esta política es aplicable a los administradores y usuarios de los sistemas de información de la AAA, así como a empleados y visitantes del Departamento de Sistemas de Información.

DEFINICIONES DE TÉRMINOS:

1. Acceso lógico – es el resultado positivo de una autenticación que permitirá al usuario entrar a su cuenta en el servidor o utilizar una aplicación hasta que ésta caduque.
2. Antivirus – una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos.
3. Contraseña – es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña tiene que mantenerse en secreto.
4. Dueño de la información – Director de Departamento o persona designada en cada departamento, responsable de los procesos e información que en su unidad se procesan.

5. "Hackers" – personas que utilizan su conocimiento para aprovecharse de los errores de los sistemas, para destruirlos, robar información, programar virus, entre otros.
6. "Screen saver" – es un programa que permite restringir el acceso a una computadora cuando está encendida y no está en uso. Para desactivarlo se requiere que el usuario entre su código de acceso y contraseña.
7. Sistemas de información - se refiere a programas, aplicaciones, dispositivos, bases de datos, redes de comunicación y archivos electrónicos.
8. "UPS" – es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

RESPONSABILIDADES:

1. El Director de Sistemas de Información es responsable de:
 - a. Implantar y, promover el cumplimiento de los controles y medidas de seguridad necesarios para minimizar los riesgos de accesos no autorizados, pérdida de información y asegurar el funcionamiento adecuado de la infraestructura y la integridad de la información contenida en ella.
 - b. Salvaguardar los sistemas de información de la AAA.
 - c. Evaluar, salvaguardar y/o eliminar toda información contenida en cualquier equipo del cual se requiera disponer.
 - d. Vigilar el cumplimiento, mantenimiento y actualización de esta política.
2. El Oficial Principal de Seguridad de Informática o su representante autorizado es responsable de:
 - a. Validar el acceso lógico a las aplicaciones con el dueño de la información del departamento o directorado afectado.
 - b. Asegurar que se cumpla con el manejo adecuado de las contraseñas utilizadas por los usuarios.

DETERMINACIÓN:

El manejo y administración de información en toda organización constituye una de las funciones más relevantes de un departamento de sistemas de Información, y por lo tanto, la seguridad de la misma es considerada como un elemento crítico en el desempeño de esta función.

Tomando en cuenta la naturaleza de negocio de la Autoridad de Acueductos y Alcantarillados (AAA), la seguridad de los recursos e infraestructura de sistemas de información cobra mayor trascendencia, por lo que es primordial el implantar medidas y controles de seguridad que minimicen los riesgos de intromisiones o accesos no autorizados.

1. Aunque la seguridad de los sistemas de información de la AAA es responsabilidad de toda la organización en su conjunto, el Departamento de Sistemas de Información juega un papel protagónico debido a que es responsable de administrar y monitorear los recursos de la AAA, y asegurar el uso correcto de los mismos. Por tal razón, el Departamento de Sistemas de Información deberá ejecutar medidas y controles de seguridad como administrador de los sistemas de información para mitigar los riesgos y salvaguardar la integridad de la información de la AAA.
 - a. Es política de la AAA el mantener la confidencialidad de los estándares técnicos de los sistemas de información con el propósito de salvaguardar la integridad de las medidas de seguridad establecidas en los mismos.
 - b. Toda actividad que se realice utilizando la infraestructura de sistemas de información de la AAA es únicamente para propósitos profesionales y ningún usuario de la misma debe tener expectativa de privacidad sobre información alguna; por lo que la AAA, a través del Departamento de Sistemas de Información, se reserva el derecho de monitorear y asegurar el cumplimiento de cualquier control y política de seguridad establecida. Cualquier acto que violente las políticas y controles establecidos deberá ser investigado y, según los hallazgos encontrados, se tomará la acción correspondiente.
 - c. Todo programa o aplicación a ser implantado en la AAA tendrá que ser evaluado y aprobado por el Departamento de Sistemas de Información.
 - d. El Departamento de Sistemas de Información no se responsabiliza por la implantación o instalación de programas o aplicaciones que no hayan sido aprobados.
 - e. La activación y desactivación de accesos lógicos a los sistemas de información de la AAA serán procesadas por el Oficial Principal de Seguridad Informática o su representante autorizado siempre que se incluya la solicitud que documente la necesidad. Cualquier modificación de acceso deberá ser autorizada por el Dueño de la Información.

- f. Toda nueva solicitud de autorización de acceso lógico a los sistemas de información de la AAA deberá ser autorizada por el Dueño de la Información del departamento al cual pertenece el empleado. Dicha solicitud deberá ser sometida al Departamento de Sistemas de Información.
2. Seguridad Física en el Departamento de Sistemas de Información y Centro de Cómputos
- a. El área de recepción del Departamento de Sistemas de Información y las salidas de emergencia deberán contar con un sistema de control de acceso físico electrónico mediante tarjeta de aproximación para restringir el acceso a personas no autorizadas.
- b. Todo empleado, contratista y/o proveedor al que no se le haya autorizado acceso físico electrónico mediante tarjeta de aproximación deberá registrarse con el Oficial de Seguridad Física designado a la entrada principal del lugar donde ubica el Departamento de Sistemas de Información.
- c. El Centro de Cómputos debe ser un área de acceso físico restringido y solamente personal debidamente autorizado tendrá acceso al mismo.
- d. Aquellas personas que necesiten realizar labores en las facilidades o equipos del Centro de Cómputos y que no tengan acceso físico mediante la tarjeta de aproximación, deberán firmar una hoja de registro de entrada y salida cada vez que ingresen o salgan del área. Además tienen que estar acompañadas en todo momento por un funcionario autorizado.
- e. El Centro de Cómputos debe contar con un sistema alternativo de generación de energía, el cual debe estar conectado a la toma principal de corriente del edificio. Sistemas de baterías o "UPS" son requeridos para evitar cualquier interrupción del servicio eléctrico.
- f. El Centro de Cómputos debe tener sus propias unidades de aire acondicionado, independientemente de si existe en el edificio un sistema de aire acondicionado central.
- g. El Centro de Cómputos debe contar con un sistema de monitoreo de temperatura y humedad para proteger los equipos instalados en el mismo. Además, debe contar con un sistema de cámaras de seguridad para monitorear la entrada y salida del personal al Centro.
- h. En la medida que sea posible, todo material utilizado en construcciones en las facilidades del Centro de Cómputos debe ser resistente al fuego. Además, el Centro de Cómputos debe ser habilitado con sistemas automáticos de detección y extinción que disminuyan las posibilidades de un incendio.

- i. Diariamente, se harán copias de resguardo (“backup”) de todos los datos contenidos en los sistemas de información, incluyendo los servidores de ambiente Windows y ambiente UNIX, según el Procedimiento 657 – Para la Creación y Manejo de Copias de Resguardo”.
 - j. Diariamente, se harán rotaciones de las copias de resguardo a una entidad externa para mitigar riesgos de pérdida de información.
 - k. Es política de la AAA realizar pruebas anuales del Plan de Recuperación de Desastres (“Disaster Recovery Plan”, “DRP”).
 - l. Los sistemas catalogados como críticos y los servicios ofrecidos por el Centro de Cómputos contarán con estrategias de recuperación ante desastre (*Disaster Recovery*), mitigando así cualquier impacto negativo a las operaciones normales del negocio.
 - m. No se hará pública la localización del Centro de Cómputos por medio de carteles ni señales con el propósito de mantener un perfil bajo de la ubicación del Centro de Cómputos.
 - n. El Centro de Cómputos no debe ser localizado en una zona inundable.
3. Seguridad en Estaciones de Trabajo, Aplicaciones y Servidores
- a. Todo desarrollo o adquisición de aplicaciones deben ser comprobadas y validadas adecuadamente contra violaciones a la seguridad en el sistema, y deben poseer un control de acceso lógico que requiera la identificación de usuario y contraseña.
 - b. El Departamento de Sistemas de Información debe mantener un mecanismo de monitoreo o registro (“log”) de accesos lógicos a los sistemas de información (aplicaciones y servidores), de forma que identifique el nombre del usuario, tiempo de acceso, fecha y hora del acceso, entre otros.
 - c. Toda conexión remota a los sistemas de información debe ser restringida únicamente a usuarios debidamente autorizados y justificados según las necesidades de su trabajo. La conexión debe estar limitada a la porción de interés y de ninguna forma un usuario debe ser permitido a acceder a más información de la que por diseño debe ser accedida.
 - d. El Departamento de Sistemas de Información debe revisar periódicamente la nueva tecnología disponible y mantenerse informado de nuevos mecanismos de control, así como de tecnología que es utilizada por *hackers* para violentar la seguridad de los controles de aplicaciones, sistemas operativos, servicios web, entre otros.

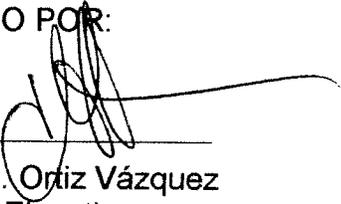
- e. Se espera que las contraseñas cumplan con los siguientes estándares establecidos en esta política, aunque se reconoce que podrían existir excepciones las cuales deben estar debidamente justificadas y documentadas. Los estándares son los siguientes:
- 1) El uso de las contraseñas es confidencial y no podrá ser compartido.
 - 2) La contraseña tendrá un largo mínimo de ocho caracteres en combinación de letras mayúsculas, minúsculas y números.
 - 3) Las contraseñas no deben ser impresas, por lo tanto no estarán guardadas en lugares visibles o de fácil acceso.
 - 4) Todas las contraseñas para las aplicaciones deberán ser cambiadas cada 90 días y no se deben reutilizar durante un periodo no menor de un año.
 - 5) La cuenta se bloqueará "*account lock*" por un periodo de 15 minutos luego de 3 intentos fallidos, ya sea que esto ocurra por un usuario regular o por alguna herramienta de escaneo de contraseñas.
 - 6) El sistema "*Active Directory*" debe estar configurado para avisar el cambio de contraseña con 5 días antes de su expiración. De no cambiarse se bloqueará automáticamente el acceso al sistema. Para acceder al sistema nuevamente, el Supervisor del usuario debe solicitar reactivar la cuenta de acceso al Departamento de Sistemas de Información.
 - 7) Se requiere que toda computadora tenga activado un "*screen saver*" con la opción de contraseña activa. El mismo debe activarse a los diez (10) minutos de inactividad.
 - 8) Se debe cambiar la contraseña inicial de los Servidores y Equipos de Comunicaciones y la misma sólo debe ser conocida por el personal designado de la Dirección Auxiliar de Servicios Informáticos del Departamento de Sistemas de Información.
 - 9) Existirán contraseñas de emergencia las cuales permitirán acceso de "Administrador" a los servidores y/o aplicaciones. Estas contraseñas permanecerán en sobre sellado y estarán guardadas en bóveda. El acceso a las mismas será sólo en momentos de una emergencia y requerirá una doble autorización al momento de ser utilizadas.
- f. Los programas de antivirus en todas las estaciones de trabajo deben ser actualizados con las definiciones nuevas de antivirus según sean provistos por el proveedor.

- g. Todo movimiento de equipo de sistemas de información debe ser autorizado por la Gerencia de Servicios Informáticos del Departamento de Sistemas de Información, según el Procedimiento 652 – “Para el Control de Inventario de Equipos de Sistemas”.
- h. Cualquier atentado a la seguridad de los sistemas de información de la AAA que haya sido detectado, será debidamente documentado y reportado inmediatamente al Oficial Principal de Seguridad Informática y al Director de Sistemas de Información para su investigación e implantación de medidas correctivas.

VIGENCIA:

Esta Orden Administrativa tiene vigencia inmediata y deja sin efecto todas las comunicaciones que se hayan cursado sobre este asunto.

APROBADO POR:



Ing. José F. Ortiz Vázquez
Presidente Ejecutivo

12/23/2011
Fecha de Aprobación