

**OFICINA DEL PRESIDENTE EJECUTIVO*****ORDEN ADMINISTRATIVA***NÚMERO: OA-2011-08DISTRIBUCIÓN: “D”FECHA: 16 de agosto de 2011**ASUNTO: POLÍTICA SOBRE RESGUARDO DE INFORMACIÓN****PROPÓSITO:**

El propósito de esta política es salvaguardar los activos de información, prevenir pérdidas en caso de fallas en los sistemas y permitir un proceso de restauración de información adecuado.

EXPOSICIÓN DE MOTIVOS:

Esta política aplica a todos los sistemas de información y los activos de información de la Autoridad.

RESPONSABILIDADES:

1. El Director de Sistemas de Información es responsable de hacer que se cumpla esta política en la Autoridad.

DEFINICIÓN DE TÉRMINOS:

1. Resguardo – copia fiel y exacta de archivos, data, programas, configuraciones y demás información considerada suficientemente importante como para ser conservada.
2. Medio del resguardo – dispositivo para guardar la data y/o aplicaciones a resguardar de acuerdo al tipo y la frecuencia definida.
3. Restauración – se refiere a las técnicas empleadas para recuperar datos y/o aplicaciones que han sido perdidos, modificados o eliminados.

DETERMINACIÓN:

1. Procedimientos de resguardo y restauración deberán ser definidos e implementados para los sistemas de información. Estos procedimientos deberán ser revisados toda vez que los sistemas sean modificados.
2. La manera en que se hacen los resguardos (incremental, diferencial, *full*) y la frecuencia de éstos (diario, semanal, mensual, anual, replicación), deben reflejar los requisitos de la AAA, los requisitos de seguridad de la información y el nivel de criticidad de la información para apoyar la continuidad de las operaciones.
3. Existirán copias de resguardo en todo momento con el fin de proteger la disponibilidad y la integridad de los activos de información.
4. Copias de resguardo deben existir antes y luego de la ocurrencia de cambios realizados en el ambiente de producción de la AAA. Esto para garantizar la integridad y disponibilidad de los activos de información.
5. Los accesos a los mecanismos de resguardo se proporcionarán basados en los roles y responsabilidades de sus administradores con el fin de proteger la información de accesos no autorizados, modificaciones o destrucción.
6. Podrán existir copias de resguardo de información tanto en medios magnéticos físicos como en medios virtuales.
7. Se utilizarán etiquetas de identificación para los medios físicos de resguardo.
8. Pruebas de los resguardos
 - a. Las pruebas de los resguardos deben ocurrir ya sea como parte de las pruebas de recuperación anuales o como parte de las pruebas a realizar durante una nueva implementación catalogada de alto impacto.
 - b. Los procedimientos de restauración deben ser probados regularmente para asegurar que los mismos están alineados con los requisitos de recuperación previamente establecidos.

9. Almacenaje de los resguardos

- a. Los resguardos deberán ser enviados periódicamente a una localidad remota que cumpla con los estándares mínimos de la industria, mitigando así el riesgo de pérdidas por causa de un desastre en el Centro de Cómputos de la AAA.
- b. Las copias de resguardo deberán estar provistas de un nivel adecuado de protección física y ambiental durante el almacenamiento temporero en el Centro de Cómputos, durante su transportación y en la localidad remota. El nivel de seguridad física y ambiental para los medios de resguardo debe ser la misma que la proporcionada a los sistemas de información.
- c. Se deberá mantener un inventario que identifique en todo momento el detalle y actividad de los medios de resguardo conforme se van creando y pasando por sus diferentes etapas o ciclo de vida útil. Este inventario deberá estar disponible en todo momento tanto en el Centro de Cómputos de la AAA como en la localidad remota.

10. Acceso a la Bóveda local de la Autoridad

- a. El acceso a la bóveda es permitido solamente a personal debidamente autorizado.
- b. El acceso a la bóveda estará controlado por mecanismos de seguridad mediante el uso de combinación de contraseñas.
- c. La combinación de contraseñas de la bóveda estará escrita y guardada en un sobre sellado. La misma estará firmada por el Gerente del Centro de Cómputos y custodiada bajo llave en la oficina del Directorado de Sistemas de Información.
- d. La combinación de contraseñas de la bóveda será reemplazada anualmente. También serán reemplazadas a causa de renuncia, reubicación a otro departamento, despido o jubilación de personal con acceso a la bóveda.

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