

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos

Fecha del informe: 21 de octubre de 2009 Periodo auditado: 1 de junio de 2007 al 30 de abril de 2008

Indique:  PAC  ICP

Funcionario enlace: Myrna Reyes Ortega Puesto: Directora – Oficina Auditoría Interna Teléfono: (787) 765-7575

Funcionario principal o su representante autorizado: Ing. Rebeca Nieves Ortega Puesto: Directora Ejecutiva Teléfono: (787) 765-7575

*Rebeca Nieves*  
 Firma del funcionario principal o su representante autorizado

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA Fecha: Enero 13, 2010.

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
2. Ejercer una supervisión efectiva sobre el Gerente de Sistemas de Información de la OSI para asegurarse de que: <ul style="list-style-type: none"> <li>a. Realice un análisis de riesgos, según se establece en la Política Núm. TIG-003. El informe, producto de este análisis de riesgos, debe ser sometido para su revisión y aprobación [Hallazgo 1-a].</li> <li>b. Revise el Plan de Seguridad para que se incluya los criterios descritos en el Hallazgo 1-b y luego lo someta para aprobación. Una vez aprobado,</li> </ul>	Se incorporó, como parte del Plan de Trabajo de la OSI, realizar un Análisis de Riesgo el cual será sometido para la revisión y aprobación. Se comenzará a trabajar a partir de enero de 2010.  Se ha incorporado en el Plan de Trabajo de la OSI:	No cumplimentada         Parcialmente cumplimentada

(Véase instrucciones al final del modelo)

Iniciales *RJ*

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040

Entidad auditada: Autoridad de Desperdicios Sólidos

Fecha del informe: 21 de octubre de 2009

Período auditado: 1 de junio de 2007

al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>asegurarse de que se realice pruebas periódicas y se divulgue a los empleados y funcionarios concernidos.</p>	<ul style="list-style-type: none"> <li>• realizar pruebas sobre la validación de las normas de seguridad;</li> <li>• realizar y evidenciar análisis de riesgos;</li> <li>• desarrollar un programa de adiestramiento especializado al equipo de seguridad y otro a empleados y contratistas.</li> <li>• Desarrollar el documento explicativo sobre la interconexión de los sistemas                         <ul style="list-style-type: none"> <li>* **</li> <li>**</li> </ul> </li> <li>• Instalar un "Firewall" más resistente y potente al existente.</li> </ul> <p>A partir de enero de 2010 se ha proyectado la realización de los puntos antes descritos. Se incluye copia del Plan de Trabajo de la OSI.</p> <p>*La ADS solo comparte información con el público mediante su portal de internet. No lo hace de forma interactiva con el público.                  **Una vez terminada todas las</p>	

(Véase instrucciones al final del modelo)

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos

Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>c. Revise el Plan de contingencia para la Recuperación de Datos y disponibilidad de los sistemas de información 2006-2007 (Plan) para que incluya los aspectos comentados en el Hallazgo 2-b.2 y lo someta, en forma final, para aprobación. [Hallazgo 2-b.1] Una vez aprobado, asegúrese de que distribuya al personal que llevará a cabo los procesos del mismo. [Hallazgo 2-b.3].</p>	<p>inclusiones al Plan de Contingencia se someterá para la aprobación y posteriormente la divulgación a los empleados y funcionarios concernidos.  Se incorporaron los requisitos para atender situaciones de emergencia. El Plan está en proceso de evaluación, aprobación y firma para luego ser distribuido al personal correspondiente.</p>	<p>Parcialmente cumplimentado</p>
<p>d. Efectúe pruebas o simulacros del Plan, por lo menos dos veces al año y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas [Hallazgo 2-b.4]</p>	<p>*La identificación del centro de procesamiento de datos alternos y de respaldo de información está en proceso de evaluación.</p>	<p>No cumplimentada</p>
<p>e. Mantenga una copia del Plan aprobado, en un lugar seguro fuera de la Autoridad. [Hallazgo 2-b.5]</p>	<p>Se ha integrado en el Plan de Trabajo para realizarse durante los meses de abril y noviembre de 2010.</p>	<p>No cumplimentada</p>
<p>f. Redacte y someta para aprobación, las normas y los procedimientos necesarios para reglamentar la producción, el almacenamiento y la conservación de</p>	<p>En proceso de identificación del lugar para someter la petición.  En proceso de redacción de los procedimientos para la generación de</p>	<p>No cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales 


**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos

Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>los respaldos y que establezca la necesidad de mantener un inventario de los medios magnéticos utilizados para los respaldos. Una vez aprobados, asegurarse de que se realicen los respaldos de acuerdo a dicha reglamentación. [Hallazgo 3-a.1) y 2)]</p> <p>g. Mantenga copia de los respaldos fuera de los predios de la Autoridad para salvaguardar los datos de ésta y de la documentación de las instalaciones y las actualizaciones realizadas a los sistemas de información. [Hallazgo 3-a.3) y b.)]</p> <p>h. Supervise las funciones del personal encargado de administrar los sistemas operativos para que configure las siguientes opciones de seguridad en éstos para:</p> <ol style="list-style-type: none"> <li>1. Activar las opciones contenidas en la pantalla de políticas de auditoría (Audit Policies) en los servidores que se mencionan en el Hallazgo 4-a.1)</li> <li>2. Restringir el horario de acceso a los recursos de la Red, según las funciones y responsabilidades de los usuarios mencionados en el Hallazgo 4-a.2)a)</li> </ol>	<p>los respaldos e inventario de los medios magnéticos.</p> <p>En proceso de identificación del lugar para someter la petición.</p> <p>Solicitud al administrador de la red para la revisión, evaluación y acción correspondiente sobre cada uno de los puntos señalados. En espera de respuesta en o antes de febrero de 2010.</p>	<p>No cumplimentada</p> <p>No cumplimentada</p>

(Véase instrucciones al final del modelo)


Iniciales 

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07      Número de unidad: 3040      Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009      Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>3. Efectúe las modificaciones necesarias para corregir las situaciones que se comentan en el Hallazgo 4-a.2)b) y del b. 1) al 2)e)</p> <p>4. Elimine, inmediatamente, las cuentas de acceso de los empleados que hayan cesado sus funciones en la Autoridad e inactive las cuentas de los empleados que estén acogidos a una licencia o en destaque en otra agencia. [Hallazgo 4-b.2)f)]</p> <p>i. Prepare para aprobación los procedimientos para la administración de la Red en los cuales se establezcan las directrices para que el personal encargado de administrar los sistemas. [Hallazgo 4-c.1]</p> <p>1. Configure la pantalla <i>Security Properties</i> para que no se eliminen los eventos registrados del servidor principal de la Red.</p> <p>2. Revise, periódicamente, los eventos registrados en el servidor principal de la Red y, de ser necesario, tome de inmediato las medidas preventivas y correctivas necesarias.</p> <p>3. Grabe el contenido del registro en un medio de almacenamiento alternativo antes que se complete la capacidad de almacenamiento del mismo en el</p>	<p>Se redactarán los procedimientos para la administración de la Red y se espera estén disponibles en o antes de febrero de 2010.</p>	<p>No cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales 

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
sistema. j. Active la opción Enable Message Tracking del sistema de correo electrónico, como medida para controlar el uso oficial de las cuentas de correo electrónico. [Hallazgo 5-a.1] k. Restrinja los derechos y privilegios para que solamente el personal clave de la Autoridad pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. [Hallazgo 5-a.2] l. Identifique y adquiera una aplicación para analizar los registros de direcciones de Internet visitadas por los usuarios y registradas en el servidor que provee dicho servicio y adiestre al encargado de administrar la Red sobre la utilización de la misma y le asigne la responsabilidad de examinar periódicamente dichos registros. [Hallazgo 5-b]	Solicitudo al administrador de la Red para la acción correspondiente. Se revisará su cumplimiento. Se evaluará, por división, el personal autorizado a recibir correos electrónicos de fuentes externas y se restringirá a aquellos que no tengan la necesidad. En proceso de identificar una aplicación y su costo para la evaluación	No cumplimentada No cumplimentada No cumplimentada
m. Prepare las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el Hallazgo 6 y someta los mismos para la aprobación del Secretario. n. Mantenga el equipo de comunicación y la distribución del cableado en lugares cerrados con llave.	Se redactarán las normas y los procedimientos necesarios para la aprobación del Secretario. Se instaló cerradura con llave.	No cumplimentada Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales *PAF*

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: T1-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>a. Revise las medidas de seguridad existentes para establecer un acceso controlado y adecuado al área de los servidores y a los cuartos de distribución del cableado de la Red. [Hallazgo 7-a.2]</p>	<p>manteniendo el cuarto seguro y cerrado.</p>	<p>Cumplimentada</p>
<p>b. Tome las medidas necesarias para asegurarse de que los contratistas estén acompañados y supervisados por el personal de la OSI cuando necesiten realizar trabajos de mantenimiento a los sistemas. Esto, de manera que se garantice un acceso controlado a las instalaciones de la OSI. [Hallazgo 7-a.3]</p>	<p>Se preparó un registro de acceso al cuarto de servidores y a los cuartos de telecomunicaciones (Registro de Visitantes).                      El acceso es controlado por personal de la OSI.</p>	<p>Cumplimentada</p>
<p>q. Prepare los procedimientos para la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios de los sistemas computadorizados y los someta para aprobación. [Hallazgo 8]</p>	<p>Se redactarán los procedimientos relacionados a las cuentas de acceso en o antes de finalizar el mes de enero de 2010.</p>	<p>No cumplimentada</p>
<p>r. Mantenga una segregación adecuada de las funciones conflictivas que realizan los analistas programadores e implante medidas de controles compensatorios que mitiguen el riesgo resultante de una falta de segregación de funciones adecuadas. [Hallazgo 9]</p>	<p>Se someterá una solicitud a Recursos Humanos para la evaluación en la segregación de funciones del personal de la OSI. Considerando que en la actualidad son solo dos los empleados de la división de OSI</p>	<p>No cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales 

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
3. Ejercer una supervisión eficaz sobre el coordinador inter agencial para el manejo de Emergencias para asegurarse de que coordine y efectúe pruebas del Plan Operacional de emergencias, por lo menos una vez al año. [Hallazgo 2-a]	Se orientará al Coordinador Inter agencial para que coordine y realice pruebas.	No cumplimentada
4. Formalizar un acuerdo escrito con otra entidad que acepte la utilización de sus equipos en casos de desastres o emergencias en la Autoridad, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. [Hallazgo 2-c]	Se utilizarán los hallazgos en el Estudio de Riesgo y el inventario de equipo, aplicaciones y datos para identificar una entidad que nos pueda ofrecer servicios en caso de desastre	No cumplimentada
5. Realizar un análisis para determinar el personal clave de la Autoridad que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, someter la lista del personal clave de la OSI. [Hallazgo 5-a.2]	Se le solicitará a cada director de división someter listado de aquellos empleados que tengan el privilegio para recibir y enviar mensajes de correo electrónico	No cumplimentada

(Véase instrucciones al final del modelo)

Iniciales *PLP*



**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07      Número de unidad: 3040      Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009      Período auditado: 1 de junio de 2007 al 30 de abril de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
6. Ejercer una supervisión eficaz sobre el Director de Asuntos Gerenciales para que se asegure de que el Director de la División de Servicios Generales establezca un registro para mantener el control de las llaves del área de los servidores y de los cuartos de distribución del cableado de la Red que mantenga bajo su custodia. [Hallazgo 7-a.4]	Se orientará al Director de Asuntos Gerenciales a establecer un registro y control de las llaves.	No cumplimentada
7. Impartir instrucciones a la Directora de Recursos Humanos de la Autoridad para que revise las descripciones del puesto de los dos analistas programadores para que las funciones de dicho puesto no sean conflictivas. [Hallazgo 9]	Se le solicitará a la Directora de Recursos Humanos la revisión de las descripciones de puesto. Se hace la salvedad de que en estos momentos contamos con un Gerente de Sistemas de Informador y un Analista Programador.	No cumplimentada
8. Asegurarse de que el Auditor Interno [Hallazgo 10] a. Establezca un programa de adiestramiento continuo para capacitar a los auditores internos de la Autoridad en las técnicas de auditoría de sistemas de información computadorizados. b. Realice las gestiones necesarias para que se	Se orientará a la Directora de la Oficina de Auditoría Interna a integrar en el programa de adiestramiento continuo cursos sobre auditoría de sistemas de información.  Se programarán auditorías internas	No cumplimentada  No cumplimentada

(Véase instrucciones al final del modelo)

Iniciales *PH*

**PLAN DE ACCIÓN CORRECTIVA**

Informe de auditoría: TI-10-07 Número de unidad: 3040 Entidad auditada: Autoridad de Desperdicios Sólidos  
 Fecha del informe: 21 de octubre de 2009 Período auditado: 1 de junio de 2007 al 30 de abril de 2008

<b>RECOMENDACIÓN</b>	<b>ACCIÓN CORRECTIVA</b>	<b>RESULTADO</b>
examine periódicamente los controles y las operaciones de los sistemas de información computarizados de la Autoridad y la seguridad y el proceso de autorización o acreditación de las aplicaciones antes de que se implanten las mismas.	como parte del Plan de Trabajo de la Oficina de Auditoría Interna.	
9. Tomar las medidas correspondientes para que la OSI le responda a la alta gerencia de la Autoridad como una unidad independiente de sus usuarios [Hallazgo 11].	Se aprobó un organigrama donde se define que la OSI le responde a la Directora Ejecutiva.	Cumplimentada