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

Indique: ☐ **PAC** ☒ **ICP -** 3

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

Funcionario principal o su representante autorizado: Lcdo. Elí E. Díaz Atienza Puesto: Director Ejecutivo Teléfono: (787) 765-7575

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 1 de febrero de 2011
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
2. Ejercer una supervisión efectiva sobre el Gerente de Sistemas de Información de la OSI para asegurarse de que:		
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].	Se reprogramó para ser desarrollado durante los meses de febrero y marzo 2011. Ver Plan de Trabajo 2011 "Plan Riesgo Simulacro que se incluye como **Anejo B**.	No Cumplimentada
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, asegurarse de que se realice pruebas periódicas y se	Se reprogramó para ser desarrollado durante los meses de febrero y marzo 2011. Ver Plan de Trabajo 2011 (Plan Riesgo Simulacro Pág. 5. y "Firewall	No Cumplimentada

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

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
divulgue a los empleados y funcionarios concernidos.	Adiestramiento que se incluye como **Anejo C**.	
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, asegurarse de que distribuya al personal que llevará a cabo los procesos del mismo. [Hallazgo 2-b.3].	Según solicitado, se presenta evidencia del envío, vía correo electrónico, del Plan de Contingencia para la Recuperación de Datos, al personal que llevará a cabo los procesos del mismo. Incluimos copia de la evidencia de dicho envío como **Anejo D.**	Cumplimentada
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]	Se reprogramó para ser desarrollado durante los meses de febrero y marzo 2011. Ver Plan de Trabajo 2011 "Plan Riesgo Simulacro que se incluyó como **Anejo B.**	No cumplimentada
f. Redacte y someta para aprobación, las normas y los procedimientos necesarios para reglamentar la producción, el almacenamiento y la conservación de 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)]	El Procedimiento para la Producción, el Almacenamiento y la Conservación de los Respaldos se incorporó en el Plan de Contingencia para la Recuperación de Datos como parte del Anejo 5 de dicho Plan. El procedimiento quedó aprobado, automáticamente, una vez se aprobó el Plan de Contingencia. Incluimos	Cumplimentada

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
	copia del Plan como **Anejo A.**	
h. Supervise las funciones del personal encargado de administrar los sistemas operativos para que configure las siguientes opciones de seguridad en éstos para: 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) 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) 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) 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)]	La Oficina de Auditoría Interna de la ADS evaluó la configuración de las opciones de seguridad en los sistemas operativos. Se incluye copia de la hoja de trabajo utilizada como **Anejo E.**	Cumplimentada

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
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] 1. Configure la pantalla *Security Properties* para que no se eliminen los eventos registrados del servidor principal de la Red. 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. 3. Grabe el contenido del registro en un medio de almacenamiento alterno antes que se complete la capacidad de almacenamiento del mismo en el sistema.	Se incorporó el "Procedimiento para la Administración de la Red" como parte de los Procedimientos del Plan de Contingencia el cual forma parte del **Anejo 5** de dicho **Plan**. Una vez aprobado dicho Plan, el procedimiento quedó automáticamente aprobado. Se incluyó copia del Plan como **Anejo A.**	Cumplimentada
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]	En la actualidad, la empleomanía con la que cuenta la ADS, por la naturaleza de sus funciones, requiere del acceso al correo electrónico de fuentes externas. Contamos con menos personal, debido a la Ley 7 y la Ley 70, por lo que es necesario hacer más con menos.	Cumplimentada

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

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
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]	Se determinó que una vez se identifique que alguno de los empleados, por la naturaleza de sus funciones, ya no le sea necesario el uso del correo electrónico de fuentes externas, se hará lo propio para restringir los derechos y privilegios.	Cumplimentada
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]	La Oficina se encuentra en proceso de identificar la aplicación correspondiente para evaluar su costo y proceder con la solicitud.	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.	Se redactó y se incorporó el "Procedimiento para la Disposición de Información y Programas" el cual incorpora la Política Núm. TIG-007 y el "Procedimiento para Solicitud, Aprobación, Creación y Cancelación de Cuentas" dentro del **Anejo 5** del **Plan** de Contingencia. Se espera por la aprobación del Secretario.	Parcialmente Cumplimentada

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
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]	Se redactó el "Procedimiento para Solicitud, Aprobación, Creación y Cancelación de Cuentas" la cual se incluye en el **Anejo 5** del Plan de Contingencia para la Recuperación de Datos que incluimos como **Anejo A.**	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 incorporó en el Plan de Trabajo de la Oficina de Sistemas de Información para evaluar una entidad adecuada a nuestras necesidades y formalizar un acuerdo.	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]	Luego de evaluar la aplicación de la Ley 7 y la Ley 70 en la Autoridad, concluimos que con el personal con el que contamos, es necesario permitir el acceso al correo electrónico a todos los empleados. Esto por la naturaleza de sus funciones.	Cumplimentada
6. Ejercer una supervisión eficaz sobre el Director de	Se incluye copia del Registro de Uso	Cumplimentada

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

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
Asuntos Gerenciales para que se asegure de que el Director Interino 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 mantenía bajo su custodia. [Hallazgo 7-a.4]	de Llaves del Área de Servidores y Cuartos de Distribución como **Anejo F.**	
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.	La Auditora Interna tomó el adiestramiento ofrecido por la ORHELA el pasado 6 de diciembre de 2010. Además se participó del Adiestramiento ofrecido a los Auditores Internos del Gobierno donde se incluyó el tema, entre otros, de Auditorías de Sistemas de Información. Se presenta copia de los certificados, evidenciando la asistencia, como **Anejo G**.	Cumplimentada
b. Realice las gestiones necesarias para que se examine periódicamente los controles y las operaciones de los sistemas de información computadorizados de la Autoridad y la seguridad y el proceso de autorización o acreditación de las	La Oficina de Auditoría Interna inició a examinar los controles de los sistemas de información evaluando el que se hayan configurado las opciones de seguridad en los	Cumplimentada

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
aplicaciones antes de que se implanten las mismas.	sistemas operativos. Se hace referencia al **Anejo E**.	

INSTRUCCIONES PARA COMPLETAR EL MODELO PLAN DE ACCIÓN CORRECTIVA

1. El funcionario a quien se le dirijan las recomendaciones, o su representante autorizado, debe completar este modelo y someterlo a la Oficina del Contralor de Puerto Rico dentro del término de noventa (90) días consecutivos, contados a partir del primer día del mes siguiente a la fecha de publicación del informe de auditoría o especial. El mismo deberá enviarse a la dirección de correo electrónico correspondiente.

2. En aquellos casos en que queden recomendaciones pendientes de cumplimentar a la fecha del primer informe, se prepararán **informes complementarios (ICP)** cada noventa (90) días, contados a partir del primer día del mes siguiente a la fecha de la notificación del resultado de la evaluación.

3. En las columnas del modelo se incluye la siguiente información:

   a. **Recomendación**: En esta columna, se detallan las recomendaciones. Las recomendaciones se presentan en el mismo orden y con el número de identificación que aparece en el informe de auditoría o especial.

   b. **Acción Correctiva**: En esta columna, se indican las medidas adoptadas o las que se proponen tomar para cumplir con las recomendaciones.

   c. **Resultado**: En esta columna, se indica el resultado de las gestiones realizadas. Las recomendaciones se clasifican como:

      - **Cumplimentadas**: Recomendaciones para las cuales se tomaron acciones correctivas y se obtuvieron los resultados deseados.
      - **Parcialmente cumplimentadas**: Recomendaciones con respecto a las cuales se han establecido medidas correctivas, pero quedan algunos asuntos pendientes.
      - **No cumplimentadas**: Recomendaciones para las cuales no se han establecido acciones correctivas.

   En cada uno de los apartados de **Acción Correctiva** y de **Resultado** deben ofrecerse datos que permitan una evaluación adecuada.

4. En dichos informes se deben establecer las razones para objetar alguna recomendación y, una descripción específica de cualquier acción correctiva alterna implantada en sustitución de la recomendación original.

5. Recomendamos que designe a un funcionario de enlace, preferiblemente de la Oficina de Auditoría Interna, para que realice el proceso relacionado con el **PAC**.