2/7

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: **TI-10-09** Número de unidad: **5010** Entidad auditada: **Administración de Compensaciones por Accidentes de Automóviles (ACAA)**

Fecha del informe: 3 de noviembre de 2009 Período auditado: 28 de noviembre de 2007 al 27 de junio de 2008

Indique: ☐ **PAC** ☒ **ICP -** 3

Funcionario enlace: Jaime I. Nogueras Arbelo Puesto: Auditor Interno Teléfono: 787-753-0964

Funcionario principal o su representante autorizado: Julio Alicea Vasallo Puesto: Director Ejecutivo Teléfono: 787-759-8989

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 18/feb/11

Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
Recomendación 4.c. El Supervisor de los administradores de redes se asegure de que: **1)** Se limite el acceso a Internet para que el personal autorizado sólo pueda acceder las páginas electrónicas que son necesarias para cumplir con sus deberes y responsabilidades, según el análisis realizado por la gerencia. **[Hallazgo 1-a.]**	Se solicitó al Director Ejecutivo la aprobación de un contrato de Servicios Profesionales que nos ayudará a resolver varios asuntos relacionados con la seguridad de sistemas computadorizados incluyendo el mencionado en el **Hallazgo 1-a. [Anejo 1]** Además, el Supervisor de Redes realiza verificaciones sobre el acceso a Internet. **[Anejo 2]**	Cumplimentada.

(Véase instrucciones al final del modelo)

3/7

PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: **TI-10-09** Número de unidad: **5010** Entidad auditada: **Administración de Compensaciones por Accidentes de Automóviles (ACAA)**

Fecha del informe: 3 de noviembre de 2009 Período auditado: 28 de noviembre de 2007 al 27 de junio de 2008

Recomendación 4.c. El Supervisor de los administradores de redes se asegure de que: **2)** Se restrinjan los derechos y los privilegios para que solamente el personal clave de la ACAA pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 1-b.]**	El Director de Informática certifica que el Supervisor de Administradores de Redes esta desarrollando un proceso de de seguridad de Windows para restringir los derechos y privilegios de enviar y recibir mensajes de correo electrónico de fuentes externas. **[Anejo 3]** Al día de hoy ya se restringieron los accesos para recibir mensajes de correo electrónico de fuentes externas.	Cumplimentada.
Recomendación 4.c. El Supervisor de los administradores de redes se asegure de que: **5)** Se realicen las gestiones necesarias para eliminar las cuentas de acceso que nunca se han utilizado. **[Hallazgo 2-c.3]**	Certificación sobre la eliminación de cuentas de acceso que nunca se han utilizado. Además, se incluye una lista de las cuentas de usuarios activos e inactivos. **[Anejo 4]**	Cumplimentada.
Recomendación 4.c. El Supervisor de los administradores de redes se asegure de que: **6)** Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos remotos mediante procedimientos de *call back*. **[Hallazgo 5]**	En la ACAA no utilizamos el sistema *call back*. Para crear accesos remotos utilizamos VPN a través de nuestra red de comunicaciones. **[Anejo 5]**	Cumplimentada.

(Véase instrucciones al final del modelo)

Iniciales: _____

Fecha: 18-2-11

PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: **TI-10-09** Número de unidad: **5010** Entidad auditada: **Administración de Compensaciones por Accidentes de Automóviles (ACAA)**

Fecha del informe: 3 de noviembre de 2009 Período auditado: 28 de noviembre de 2007 al 27 de junio de 2008

Recomendación 4.d. Prepare y someta para aprobación: **1)** El procedimiento para la creación, el mantenimiento y el control de las cuentas de acceso a la Red de la ACAA y a Internet. En éste se debe establecer la utilización de un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas de acceso de los usuarios. **[Hallazgo 2-d.]**	Se les notificó a todos los Directores Ejecutivos Auxiliares y Directores Regionales la implantación del formulario establecido para la solicitud, aprobación, creación y cancelación de las cuentas de acceso de los usuarios. Además, se incluye copia del formulario. **[Anejo 6]**	Cumplimentada.
Recomendación 4.e. Tome las medidas necesarias para que el registro de accesos producido por el sistema electrónico de control de acceso sea revisado periódicamente. **[Hallazgo 3-a.]**	Se incluye copia de las instrucciones impartidas para la revisión del registro de acceso al Centro de Cómputos según lo establece el Procedimiento. **[Anejo 7]**	Cumplimentada.
Recomendación 4.f. Se cumpla con las disposiciones establecidas en las **Normas de Acceso y Controles de Seguridad del Centro de Cómputos: Cuarto de Operaciones, Almacén y Bóveda Interna (Norma de Acceso),** aprobadas el 29 de noviembre de 2004 por la Directora Ejecutiva de la ACAA, referentes a las medidas para controlar el acceso al Centro de Cómputos y a la Biblioteca. **[Hallazgo 3-b. y c.]**	Se incluye evidencia de los Registro de Entrada y Salida a la Directoría de Informática y el Centro de Cómputo debidamente cumplimentados según lo establece el Procedimiento. **[Anejo 8]**	Cumplimentada.

(Véase instrucciones al final del modelo)

Iniciales: [illegible]

Fecha: 18-2-11

5/7

PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: **TI-10-09** Número de unidad: **5010** Entidad auditada: **Administración de Compensaciones por Accidentes de Automóviles (ACAA)**

Fecha del informe: 3 de noviembre de 2009 Período auditado: 28 de noviembre de 2007 al 27 de junio de 2008

Recomendación 4.h. Almacene una copia de los manuales de operación de todos los sistemas del DI, y de la documentación de las aplicaciones y de los programas en el centro de respaldo externo. **[Hallazgo 8-a.6]**	El Director de Informática preparó una Certificación referente al almacenamiento de los sistemas y la documentación de las aplicaciones y los programas en el centro de respaldo externo. **[Anejo 9]**	Cumplimentada.
Recomendación 5 Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus equipos en caso de desastres o emergencias en la ACAA, 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 el DI. **[Hallazgo 7]**	El Director de Informática preparó una Certificación e incluyó evidencia de las gestiones que a realizado para conseguir facilidades para la creación de un Centro Alterno de Procesamiento. **[Anejo 10]** Debido a la importancia y complejidad de conseguir un centro alterno en caso de desastres, y lo costoso de su implantación, solicitamos se dé por cumplimentada esta recomendación. Evidenciamos las gestiones realizadas para el cumplimiento de la misma y la implantaremos tan pronto nuestra situación económica lo permita. Su cumplimiento podrá corroborarse en una futura auditoría.	Cumplimentada.

(Véase instrucciones al final del modelo)

Iniciales: _____

Fecha: 18-2-11