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.j. Establezca, un itinerario formal para proveer el servicio de mantenimiento preventivo requerido para los equipos computadorizados de acuerdo con las especificaciones de los manufactureros de éstos. **[Hallazgo 10]**	El servicio de mantenimiento de nuestros equipos computadorizados esta contratado a compañías privadas. **[Anejo 13 y 14]**	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]**	Se solicitó propuesta y las mismas se analizarán basadas en nuestros recursos económicos.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAY

Fecha: 28-10-2010

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.g. Establezca las medidas de seguridad necesarias para controlar el acceso a los cuartos de distribución del cableado de la Red y proteger los equipos de telecomunicaciones, de manera que no estén accesibles al personal ajeno a las operaciones de la Red, y que los mismos se encuentren libres de materiales inflamables y de cualquier otro tipo de material que no esté relacionado con el funcionamiento de ésta. **[Hallazgo 4]**	Se incluye Certificación de las medidas de seguridad que se establecieron. **[Anejo 10]** y copia de la Hoja de "Registro de Visitantes del Cuarto de Comunicaciones y Manejadoras de Aire" **[Anejo 11]**	Cumplimentada
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]**	Se cumple con las Normas para la Seguridad de los Datos. **[Anejo 8]**	Cumplimentada
Recomendación 4.i. Establezca, en coordinación con el Director de Recursos Humanos, un plan para ofrecer adiestramientos sobre el manejo y la operación de los equipos de prevención y de extinción de incendios, de manera que se cumpla con lo establecido en las **secciones de la 12.4 a la 12.6 del Reglamento de Personal para los Empleados Gerenciales de la ACAA**, aprobado el 19 de julio de 2005 por la Junta de Directores. **[Hallazgo 9-a.3)]**	Se estableció un Plan de Adiestramiento en coordinación con la Directoría de Recursos Humanos. **[Anejo 12]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV
Fecha: 28-10-2010

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

4) El procedimiento de respaldos que describa, entre otras cosas: el proceso de respaldar la información y los programas, y para probar periódicamente los respaldos; el ciclo de reutilización, la rotulación y el almacenamiento de las cintas de respaldos; y la producción de un registro detallado sobre el contenido y el movimiento de éstas. **[Hallazgo del 8-a.1) al 5)]**	Se cumple con las Normas para la Seguridad de los Datos. **[Anejo 8]**	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 cumple con el Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	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 cumple con el: • Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]** • Normas para el Control de Acceso al Centro de Cómputos, y a las Áreas del Equipo de Comunicaciones y Cableado **[Anejo 9]** • Normas para la Seguridad de los Datos. **[Anejo 8]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAY

Fecha: 28-10-2010

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

6) Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos remotos mediante procedimientos de *call back*. **[Hallazgo 5]**	Se sacaron los que no debían estar y solo se da acceso remoto basado en necesidades especiales, según se establece en el Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	Cumplimentada
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 cumple con el Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	Cumplimentada
2) Los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. **[Hallazgo 5]**	Se cumple con el Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	Cumplimentada
3) El **Plan de Contingencias** en el que se incluyan los procedimientos para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información de acuerdo con los criterios que se mencionan en el **Hallazgo 6**.	Se incluye copia de la Hoja de Trámite enviada a la Oficina del Contralor de PR el 7 de octubre de 2010, para el cumplimiento de esta recomendación. **[Anejo 7]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 28-10-2010

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

b) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la Red. **[Hallazgo 2-a.2]**	El cumplir con esta recomendación será a largo plazo debido a que requiere modificaciones de configuración en nuestro sistema y requiere contratación de servicios de consultoría.	Cumplimentada
f) Establecer una fecha de expiración para las contraseñas de las cuentas de acceso. **[Hallazgo 2-c.2]**	A pesar de los esfuerzos que se hicieron para establecer fecha de expiración para las contraseñas de las cuentas de acceso determinamos que no es posible por las dificultades que presentó y conllevaría un gasto económico excesivo. **[Anejo 6]**	Cumplimentada
Recomendación 4.c. El Supervisor de los administradores de redes se asegure de que: **4)** Se activen las opciones correspondientes en la pantalla de políticas de auditoría *(Audit. Policies)* que se mencionan en el **Hallazgo 2-b.**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la ACAA.	No tenemos espacio en disco. Se trabajará a largo plazo según nos lo permitan nuestras finanzas. Requiere consultoría externa.	Cumplimentada
5) Se realicen las gestiones necesarias para eliminar las cuentas de acceso que nunca se han utilizado. **[Hallazgo 2-c.3]**	Se realiza por comunicación del área de trabajo, según lo establece el Procedimiento para el Control de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 28-10-2010

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.]**	Se envió comunicación escrita al Administrador de Redes para que restrinja los derechos y privilegios para que solamente el personal clave de la ACAA pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según indicado en la comunicación recibida. **[Anejo 3]**	Cumplimentada
3) Se efectúen las modificaciones en los parámetros de seguridad de los servidores de la Red para: a) Restringir el horario de acceso a los recursos de la Red, según las funciones y las responsabilidades de cada usuario, y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la Red fuera de horas laborables. **[Hallazgo 2-a.1]**	Se envió comunicación escrita al Administrador de Redes para que establezca los parámetros para restringir el horario de uso de la Red de 7:00 a.m. a 5:00 p.m., según las funciones y responsabilidades de cada usuario. **[Anejo 4]** Se envió notificación a los Directores de las Directorías y Oficinas Regionales en relación a dicho asunto. **[Anejo 5]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV
Fecha: 28-10-2010

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 3 Realizar un análisis para determinar el personal clave de la ACAA que requiere tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, someter la lista del personal clave al DI. **[Hallazgo 1-b.]**	Se envió comunicación a los directores de cada oficina solicitando los privilegios para enviar y recibir mensajes de correo electrónico necesarias para cada tipo de trabajo. Se analizó y se dio acceso externo a aquellos indicados en la lista recibida. **[Anejo 1]**	Cumplimentada
Recomendación 4 Ejercer una supervisión efectiva sobre el Director del DI para asegurarse de que: **Recomendación 4.a.** Se efectúen inspecciones periódicas necesarias para verificar el uso oficial de las cuentas para acceder a Internet y al correo electrónico. **[Hallazgo 1]**	Se está monitoreando el uso de la Internet y los correos electrónicos, según lo establece el Procedimiento para el Control de Cuentas de Accesos a los Sistemas Computadorizados. **[Anejo 2]**	Cumplimentada
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 envió comunicación escrita al Administrador de Redes para que de acceso a los empleados solamente, a las páginas indicadas en la comunicación recibida. **[Anejo 3]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 28-10-2010

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 -** 2

Funcionario enlace: Zamary Solivan Cartagena Puesto: Auditora Interna 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: 28-10-2010

Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
Recomendación 2 Realizar un análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado para acceder a Internet. Luego de efectuado el análisis, someter la lista de las páginas autorizadas al DI. **[Hallazgo 1-a.]**	Se envió comunicación a los directores de cada oficina solicitando las páginas electrónicas necesarias para cada tipo de trabajo. Se analizó y se dio acceso a las páginas indicadas en la comunicación recibida. **[Anejo 1]**	Cumplimentada