



**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** - \_\_\_\_\_

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

  
 Firma del funcionario principal o su representante autorizado

Fecha: 26/feb/10

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p><b>Recomendación 2</b>            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.]</p>	<p>Se prepararon listas por Directorías, los directores establecieron quienes serían los empleados que utilizarán las páginas electrónicas según sus deberes y se le dio acceso a sólo esos empleados autorizados. Dichas listas están en evaluación por el Director de DI.</p>	<p>Parcialmente Cumplimentada</p>



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

<p><b>Recomendación 3</b> 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.]</p>	<p>Las Directorías están preparando una lista de los empleados con los correos electrónicos de fuentes externas para ser programados en el sistema.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4</b> Ejercer una supervisión efectiva sobre el Director del DI para asegurarse de que:</p> <p><b>Recomendación 4.a</b> Se efectúen inspecciones periódicas necesarias para verificar el uso oficial de las cuentas para acceder a Internet y al correo electrónico. [Hallazgo 1]</p>	<p>Se incluirá como parte del Plan de Seguridad.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.b</b> Se ofrezcan las orientaciones a los usuarios de los sistemas computarizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de Internet y del correo electrónico. [Hallazgo 1]</p>	<p>Cuando los empleados comienzan a trabajar en nuestra agencia se les hace entrega de las <b>Normas sobre el uso de los Sistemas Electrónicos en la ACAA</b>. Además, el 24 de noviembre de 2009 el Director Ejecutivo sometió memorando a todo el personal sobre el cumplimiento del mismo. [Anejo 1]</p>	<p>Cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales: ASL

Fecha: 26 feb. 10



**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:

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.]**

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.]**

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]**

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]**

Se incluyeron solamente las autorizadas por las Directorías y se está evaluando una aplicación que permita acceder las páginas que son necesarias.

La mensajería a fuentes externas está configurada parcialmente.

No está configurado. Se incluirá un control del horario normal de trabajo.

No está configurado. Se está trabajando para ponerlo en función.

Parcialmente Cumplimentada

Parcialmente Cumplimentada

Parcialmente Cumplimentada

Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: ASL

Fecha: 26/feb/10



**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

<p>c) Requerir un mínimo de 10 días antes de que el sistema permita al usuario cambiar la contraseña nuevamente. <b>[Hallazgo 2-a.3]</b></p>	<p>Está en un mínimo de 10 días antes que el usuario pueda cambiar su contraseña. <b>[Anejo 2]</b></p>	<p>Cumplimentada</p>
<p>d) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas. <b>[Hallazgo 2-a.4]</b></p>	<p>Es ocho caracteres, con mayúscula, minúscula y números. <b>[Anejo 2]</b></p>	<p>Cumplimentada</p>
<p>e) Requerir a los usuarios cambiar sus contraseñas en un término fijo de, por lo menos, una vez al año. <b>[Hallazgo 2-c.1]</b></p>	<p>Se tiene que cambiar la contraseña cada cuarenta y cinco (45) días.</p>	<p>Cumplimentada</p>
<p>f) Establecer una fecha de expiración para las contraseñas de las cuentas de acceso. <b>[Hallazgo 2-c.2]</b></p>	<p>No configurado. Se está evaluando.</p>	<p>Parcialmente Cumplimentada</p>
<p>4) Se activen las opciones correspondientes en la pantalla de políticas de auditoría (<i>Audit. Policies</i>) 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.</p>	<p>No configurado. En el análisis se comprobó que esto utiliza mucho espacio en discos y no tenemos dicho espacio disponible en este momento. Hay que determinar por cuanto tiempo se van a guardar las actividades.</p>	<p>Parcialmente Cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales:

Fecha:

*[Handwritten Signature]*  
 20 feb. 10



### 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

Periodo auditado:

28 de noviembre de 2007

al

27 de junio de 2008

<p>5) Se realicen las gestiones necesarias para eliminar las cuentas de acceso que nunca se han utilizado. <b>[Hallazgo 2-c.3]</b></p>	<p>Se preparó un procedimiento para controlar los accesos a los sistemas computadorizados. <b>[Anejo 3]</b> Este Procedimiento esta en revisión por el Comité de Normas y Procedimientos para la aprobación del Director Ejecutivo.</p>	<p>Parcialmente Cumplimentada</p>
<p>6) Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos remotos mediante procedimientos de <i>call back</i>. <b>[Hallazgo 5]</b></p>	<p>El número limitado de usuarios no se ha configurado.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.d</b></p> <p>Prepare y someta para aprobación:</p> <p>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. <b>[Hallazgo 2-d.]</b></p> <p>2) Los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. <b>[Hallazgo 5]</b></p>	<p>Se continúa trabajando con las medidas correctivas para cumplir con esta recomendación.</p> <p>Se continúa trabajando con las medidas correctivas para cumplir con esta recomendación.</p>	<p>Parcialmente Cumplimentada</p> <p>Parcialmente Cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales:

Fecha:

20 feb/10



**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

Periodo auditado:

28 de noviembre de 2007

al

27 de junio de 2008

<p>3) El <b>Plan de Contingencias</b> 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 <b>Hallazgo 6</b>.</p>	<p>El Director Ejecutivo aprobó el Plan de Contingencia, Versión 1.</p>	<p>Cumplimentada</p>
<p>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. [<b>Hallazgo del 8-a.1) al 5)</b>]</p>	<p>Se continúa trabajando con las medidas correctivas para cumplir con esta recomendación.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.e</b>        Tome las medidas necesarias para que el registro de accesos producido por el sistema electrónico de control de acceso sea revisado periódicamente. [<b>Hallazgo 3-a.</b>]</p>	<p>Se están identificando recursos adicionales para poder cumplir con esta recomendación.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.f</b>        Se cumpla con las disposiciones establecidas en las <b>Normas de Acceso y Controles de Seguridad del Centro de Cómputos: Cuarto de Operaciones, Almacén y Bóveda Interna (Norma de Acceso)</b>, 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. [<b>Hallazgo 3-b. y c.</b>]</p>	<p>Se estableció un procedimiento y se incluirá al procedimiento de accesos, para que todo personal que entra al Centro de Cómputos se registre. Ese registro lo verificará semanalmente el Supervisor del Centro de Cómputos. [<b>Anejo 4</b>] Este Procedimiento esta en revisión por el Comité de Normas y Procedimientos para la aprobación del Director Ejecutivo.</p>	<p>Parcialmente Cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales:

Fecha:

26/feb/10



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

Anejo  
Página 7 de 8

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:

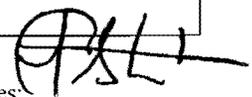
28 de noviembre de 2007

al

27 de junio de 2008

<p><b>Recomendación 4.g</b></p> <p>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. <b>[Hallazgo 4]</b></p>	<p>Estamos en proceso de preparar el procedimiento.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.h</b></p> <p>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. <b>[Hallazgo 8-a.6]</b></p>	<p>Estamos en la búsqueda de un centro de respaldo.</p>	<p>Parcialmente Cumplimentada</p>
<p><b>Recomendación 4.i</b></p> <p>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 <b>Reglamento de Personal para los Empleados Gerenciales de la ACAA</b>, aprobado el 19 de julio de 2005 por la Junta de Directores. <b>[Hallazgo 9-a.3]</b></p>	<p>Se está coordinando con Recursos Humanos llevar a cabo los adiestramientos.</p>	<p>Parcialmente Cumplimentada</p>

(Véase instrucciones al final del modelo)

Iniciales: 

Fecha: 26 Feb. 10



### 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>Recomendación 4.j</b>  Se establezca un itinerario formal para proveer el servicio de mantenimiento preventivo requerido para los equipos computarizados de acuerdo con las especificaciones de los fabricantes de éstos. <b>[Hallazgo 10]</b>	Los fabricantes con contratos de mantenimiento brindan este servicio.	Cumplimentada
<b>Recomendación 5</b>  Formalizar un acuerdo escrito con un centro externo que acepte la utilización de sus equipos en caso de desastres o emergencias en la ACAA, o considerar establecer su propio centro externo en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra el DI. <b>[Hallazgo 7]</b>	Estamos en la búsqueda de un centro externo.	Parcialmente Cumplimentada
<b>Recomendación 6</b>  Ejercer una supervisión efectiva sobre el Director de Administración de Propiedades para que se asegure de que los equipos de prevención y de extinción de incendios ubicados en el Centro de Cómputos del DI sean inspeccionados conforme a las regulaciones aplicables a los mismos. <b>[Hallazgo 9-a.1) y 2)]</b>	La oficina de Auditoría Interna inspeccionó los extintores del área de Centro de Cómputos y los mismos fueron certificados en septiembre de 2009 y tienen una fecha de vencimiento de septiembre de 2010. La compañía Fire Safe, Inc. sometió como evidencia un reporte de la inspección realizada al sistema de incendios FM 200 Kidde Scorpio. <b>[Anejo 5]</b>	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales:

Fecha: 20 / feb. / 10