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 -** 1

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: 22 jun. 10
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.]**	El Director Ejecutivo Auxiliar de la Directoría de Informática realiza una evaluación de la lista entregada por los directores para determinar que páginas electrónicas se autorizarán al personal, según deberes y responsabilidades del empleado.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

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.]**	El Director Ejecutivo Auxiliar de la Directoría de Informática realiza una evaluación de la lista entregada por los directores para determinar el personal que se le dará acceso para enviar y recibir mensajes de correo electrónico de fuentes externas.	Parcialmente 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]**	Estamos evaluando la posible compra de una aplicación para monitorear el uso del Internet y los correos electrónicos. En adición esto conlleva una nueva plaza para el monitoreo.	Parcialmente 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.]**	Véase Medidas Correctivas de la **Recomendación 2.**	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 22 jun. 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: **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.]**	Véase Medidas Correctivas de la **Recomendación 3.**	Parcialmente 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]** 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]** f) Establecer una fecha de expiración para las contraseñas de las cuentas de acceso. **[Hallazgo 2-c.2]**	Estamos evaluando la posible compra de una aplicación para monitorear el uso del Internet y los correos electrónicos. En adición esto conlleva una nueva plaza para el monitoreo. Se intentó hacer una configuración con el apoyo de Consultores de Seguridad de Redes y resultó en muchos errores del Sistema. Se requiere configurar de nuevo el Sistema de Seguridad, cuyo inversión en recursos humanos y económicos es alto.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAY

Fecha: 22 jun. 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: **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.	Se está analizando varias opciones relacionadas para determinar si se pueden usar discos externos y aumentar la capacidad de los discos duros o limitar los días en el que se acumulen los datos.	Parcialmente Cumplimentada
5) Se realicen las gestiones necesarias para eliminar las cuentas de acceso que nunca se han utilizado. **[Hallazgo 2-c.3]**	Las cuentas actualmente se deshabilitan. Se eliminarán las cuentas en intervalos de seis (6) meses.	Parcialmente Cumplimentada
6) Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos remotos mediante procedimientos de *call back*. **[Hallazgo 5]**	Los accesos remotos se llevan a cabo por personal técnico y algunos consultores que tenemos debidamente identificados. Se revisará la cantidad de usuarios que actualmente tienen esta opción.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 22 jun. 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.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 sometió al Comité de Normas y Procedimientos el Procedimiento para la revisión y aprobación del Director Ejecutivo.	Parcialmente Cumplimentada
2) Los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. **[Hallazgo 5]**	Se enmendará el Procedimiento de Control de Acceso para que incluya a los usuarios remotos.	Parcialmente 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**.	El 21 de octubre de 2009, el Director Ejecutivo aprobó el Plan de Contingencia. **[Anejo 1]**	Cumplimentada
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)]**	Estamos preparando el Procedimiento que incluya las pruebas para establecer los datos. Se creará un ambiente de pruebas.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 22 jun. 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.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 impartirán instrucciones para la revisión semanal del Registro de Acceso.	Parcialmente 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 sometió al Comité de Normas y Procedimientos el Procedimiento para el Control de Acceso al Centro de Cómputos.	Parcialmente Cumplimentada
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 coordina con la Directoría de Servicios Generales las opciones para cumplir con esta recomendación.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 22 jun. 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.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 solicitarán cotizaciones de Centros de Almacenamiento.	Parcialmente 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 coordinará con la Directoría de Recursos Humanos ofrecer adiestramientos sobre el manejo y la operación de los equipos de prevención y de extinción de incendios.	Parcialmente Cumplimentada
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]**	Se preparó una directriz al personal para revisar los extintores cada tres meses dentro de los primeros cinco (5) días. **[Anejo 2]**	Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAY

Fecha: 22 jun. 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 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]**	Hemos visitado varios suplidores de centros alternos y estamos en el proceso de solicitar cotizaciones.	Parcialmente Cumplimentada

(Véase instrucciones al final del modelo)

Iniciales: JAV

Fecha: 22 jun 10