

Gobierno de Puerto Rico

Administración de Compensaciones por Accidentes de Automóviles

Procedimiento para el Control de Accesos a los Sistemas Computadorizados	
Directoria de Informática	Número:
	Nueva Creación: (X) Fecha: 11 de octubre de 2010
Fecha Efectividad:	Revisión: ()
Aprobado por :	Fecha:
 Julio Alicea Vasallo Director Ejecutivo	Enmienda: () Fecha:

Introducción -

La Administración de Compensaciones por Accidentes de Automóviles (ACAA) cuenta con una Directoria de Informática (DI). Parte fundamental de la misión de esta Directoria, para con los usuarios de los equipos y aplicaciones computadorizadas de la Agencia, es; garantizar la seguridad, buen uso y manejo de la información que se transmite por las redes cibernéticas, proveer un acceso seguro, rápido y eficiente, proveer orientación y evaluación para la automatización de los procesos, y cumplir con las especificaciones de los usuarios al otorgar los accesos a las aplicaciones y equipos computadorizados.

Propósito -

Con esta misión presente se establece este procedimiento, el cual organiza y detalla los procesos que garantizarán la seguridad y el buen manejo de la información de la Agencia, proveerá un acceso rápido, eficiente y ordenado a los usuarios, y la

orientación precisa para la automatización de los procesos de trabajo cumpliendo siempre con los criterios establecidos para otorgar los accesos a los diferentes programas y equipos utilizados en la Agencia.

Alcance -

Este procedimiento aplica a los empleados de la DI de la ACAA, y a la instalación de programas de los sistemas operativos de Redes y de estaciones de trabajo (PC). Aplica también a todo el personal especializado que ofrece servicios bajo contrato con la ACAA.

Procedimiento -

I. Ingreso de Usuarios al Sistema

1. La Directoria de Recursos Humanos solicitará a la Directoria de Informática, mediante correo electrónico, que se añada un nuevo usuario en la red de comunicaciones cibernética de la Agencia. En dicha solicitud deberá especificar:
 - a. Nombre completo del empleado con los dos apellidos
 - b. Directoria u Oficina Regional a la que pertenecerá el empleado
 - c. Carácter del nombramiento: regular o temporero
 - d. De ser temporero deberá especificar la fecha de terminación del contrato
2. La Directoria de Informática procederá a crear la cuenta del usuario, esperando por las instrucciones del Director Ejecutivo Auxiliar (DEA) o el Director de la Oficina Regional (DOR) que corresponda para proceder a definir los accesos a las aplicaciones que utilizará el usuario según las funciones asignadas.

II. Eliminación de Acceso de los Usuarios al Sistema.

1. La Directoria de Recursos Humanos notificará, mediante correo electrónico, cuando un empleado se separe de sus labores a la Directoria de Informática. En dicho comunicado deberá especificar:
 - a. Nombre completo del empleado con los dos apellidos

- b. Directoria u Oficina Regional en la que el usuario ceso sus labores
 - c. Fecha de efectividad del cese o separación del usuario
2. La Directoria de Informática procederá a desactivar la cuenta del usuario según la fecha indicada en el comunicado. La cuenta del usuario quedará desactivada por un periodo de un año, al cabo del cual se eliminará definitivamente la cuenta de los sistemas en los que fue definido el acceso del usuario y todos aquellos elementos cibernéticos relacionados.

III. Cambios a Usuarios Activos en los Sistemas

1. La Directoria de Recursos Humanos notificará, mediante correo electrónico a la Directoria de Informática el cambio de un usuario de su lugar de trabajo. En dicho comunicado deberá especificar:
- a. Nombre completo del empleado con los dos apellidos
 - b. Directoria u Oficina Regional a la que pertenece el empleado
 - c. Directoria u Oficina Regional a la que pertenecerá el empleado
 - d. Carácter del cambio del usuario, permanente o temporero
 - e. De ser temporero, indicar la fecha de terminación del cambio
2. La Directoria de Informática procederá a realizar los cambios en la cuenta del usuario, esperando por instrucciones del Director Ejecutivo Auxiliar (DEA) o el Director de la Oficina Regional (DOR) correspondiente para proceder a definir los nuevos accesos a las aplicaciones que utilizará el usuario según las funciones asignadas.

IV. Reglas Generales para la Creación, Eliminación y Modificación de Cuentas en las Aplicaciones

1. Autorización de Acceso

- a. Las solicitudes para transacciones con los accesos otorgados a los usuarios deberán ser autorizados por el Director Ejecutivo Auxiliar (DEA) o por el Director de la Oficina Regional (DOR).
- b. Los DEA'S o los DOR'S podrán delegar en un empleado designado la solicitud de cambios a los accesos. Esta delegación deberá ser validada mediante un comunicado a la Directoria de Informática. Todas las solicitudes de cambios a los accesos deberán ser realizadas utilizando

el formulario "*Documento de Solicitud de Accesos*" (Anejo A). Las comunicaciones referentes a la creación, eliminación o modificación de cuentas deberán de ser enviadas a DEA de la Directoria de Informática copiando a la cuenta de correo electrónico denominada "*Solicitud de Servicio a los Administradores de Redes*".

2. Responsabilidades

- a. El DEA de la Directoria de Informática será responsable de autorizar las solicitudes de creación, eliminación o cambio a los accesos de los usuarios a los sistemas y equipos computadorizados.
- b. Los DEA'S y los DOR'S serán responsables de autorizar en sus áreas de trabajo los accesos que se le otorgarán a los usuarios a los sistemas y equipos.
- c. El Supervisor de Redes y los Administradores de Redes serán las personas responsables de procesar aquellas solicitudes de creación, eliminación o cambio a los sistemas luego de aprobadas por el DEA de la Directoria de Informática.
- d. El Administrador de Redes al que se le asigne la tarea será responsable de imprimir el correo electrónico mediante el que se solicitó el acceso, en la ausencia de un Administrador de Redes el Supervisor de Redes realizará las funciones solicitadas en el comunicado.
- e. Previo a realizar el trabajo en los accesos o cambios a estos el Administrador de Redes al que le fue asignada la tarea será responsable de verificar que la solicitud fue emitida por el personal autorizado.
- f. El Bibliotecario será el responsable de la Bóveda del Centro de Cómputos y del control de las copias de cintas, programas y archivos digitalizados.

3. Proceso de Crear, Eliminar o Modificar Cuentas en los Sistemas

- a. Se verifica la validez de la solicitud
- b. El personal designado procesa la solicitud según los requerimientos establecidos en el comunicado

c. Si la solicitud no es validada el personal designado se comunicará con el solicitante quien deberá consultar con el DEA o DOR para preparar nuevamente la solicitud para el debido proceso y autorización.

4. Firma y Archivo de la Solicitud

a. Luego de procesada la solicitud el personal designado firmará como realizada la tarea y mantendrá en un archivo por un periodo de un año a la fecha de su creación.

b. Luego de este periodo de tiempo solicitará la disposición de estos documentos según los procedimientos establecidos por el Programa de Administración de Documentos Públicos de la ACAA.

5. Verificación de Accesos Otorgados con las Oficinas Regionales y la Directoria de Recursos Humanos

a. Una vez al año la Directoria de Informática rendirá un informe a cada DEA y DOR detallando los accesos otorgados a los usuarios de sus correspondientes oficinas.

b. El propósito de este informe será verificar la autorización de los accesos trabajados y si estos continúan vigentes. El DEA o DOR verificará el contenido del informe y actualizará el mismo de ser necesario, identificando los cambios a los usuarios que así lo requieran.

c. Una vez al año la Directoria de Informática enviará un Informe de Cuentas Activas en los Sistemas Computadorizados a la Directoria de Recursos Humanos. El propósito de este informe será identificar aquellas cuentas que continúan activas a pesar de que los usuarios de las mismas han sido separado de dichas funciones.

d. La Directoria de Recursos Humanos informará a la Directoria de Informática aquellas cuentas en el sistema que haya que modificar o eliminar.

6. Accesos por Aplicaciones –

a. El procedimiento para modificar u otorgar acceso a las diferentes aplicaciones dependerá de los parámetros establecidos para el control de los accesos de dicha aplicación. A continuación detallamos los controles según la aplicación:

i. Internet

Los accesos a la red internacional se dividen en limitados e ilimitados. El acceso a los limitados permitirá al usuario acceso a sitios en específico de la red según su DEA o DOR lo haya solicitado. En el caso de acceso ilimitado el usuario tendrá acceso a la red internacional sin límite de tiempo ni de horario, y podrá navegar a cualquier sitio dentro de la red.

ii. ACAA 21

Cuando se soliciten accesos para esta aplicación el DEA o el DOR deberá de especificar las áreas de la aplicación donde el usuario tendrá acceso y como será su presencia en la aplicación, como por ejemplo; a modo de consulta, como oficial, oficinista o supervisor.

iii. Health Trio

Cuando el DEA o el DOR solicite acceso para un empleado a esta aplicación deberá de especificar que tipo de acceso tendrá; de supervisor, o de operador.

iv. AS/400 - GHIAS

Cuando el DEA o el DOR soliciten acceso para un empleado deberá especificar en detalle las opciones a las que se autorizará al usuario. En la solicitud indicará en los encasillados a los que corresponde cada una de las opciones autorizadas.

v. GHIAS-PC (Pago Médico-Hospitalario)

Cuando el DEA o el DOR soliciten acceso para un empleado deberá especificar en detalle las opciones a las que se autorizará al usuario. En la solicitud indicará en los encasillados a los que corresponde cada una de las opciones autorizadas, se deberá indicar si el acceso es a modo de consulta (solo para ver la información) o a modo de actualización.

vi. Pagos

Cuando un DEA o un DOR soliciten acceso para un empleado deberá especificar si el acceso es solo para ver información ("view") y especificar cualquier otra opción a la que autorizará al empleado acceso. En la solicitud indicará en los encasillados a los que corresponde cada una de las opciones autorizadas.

vii. Recobro

Cuando un DEA o un DOR soliciten acceso para un empleado deberá especificar en detalle las opciones a las que autorizará al empleado acceso. En la solicitud indicará en los encasillados a los que corresponde cada una de las opciones autorizadas, como por ejemplo: Rol, Transacciones y Planes de Pago.

viii. Ley 159

Cuando un DEA o un DOR soliciten acceso para un empleado para el programa Ley 159 deberá marcar el encasillado que así indica en el documento de solicitud.

ix. AS/400 – Sistema Financiero

Cuando un DEA o un DOR soliciten acceso para un empleado para el Sistema Financiero deberá indicar en el empleado en el documento de solicitud. Indicará en los encasillados correspondientes de cada una de las opciones autorizadas. Como por ejemplo: creación de requisiciones, aprobación de requisiciones, sistema de cuentas por cobrar, sistema de cuentas por pagar, mayor general, etc. También deberá especificar: las pantallas, por ejemplo AR505, AR560, AR595, AP321, AP645, ver cuentas de presupuesto, etc., y si el acceso será a modo de consulta o a modo de actualización.

x. Acceso Físico a la Directoría de Informática

Cuando un DEA o un DOR soliciten acceso para un empleado a alguna de las áreas controladas por la Directoría de Informática se solicitará al DEA de la Directoría de Informática indicando lo siguiente:

- A. Nombre y apellidos del empleado al que se le otorgará el acceso
- B. Número del código de barra que está en la parte posterior izquierda de la tarjeta de identificación del empleado
- C. Las áreas específicas a las que se le autorizará acceder:
 - 1. Administración
 - 2. Programación
 - 3. Centro de Cómputos
 - 4. Control de Documentos y Microfilmación

xi. Razones por la que solicita el acceso

Cuando se solicite acceso para consultores, auditores o un funcionario de mayor jerarquía que el DEA de la Directoria de Informática deberá ser solicitado mediante comunicado escrito al DEA de la Directoria de Informática, por conducto del Director Ejecutivo de la ACAA. En dicho comunicado deberá especificar que tipo de acceso se otorgará, y éste deberá regirse de acuerdo a las áreas contractuales y las funciones en la Directoria.

7. Roles de los Oficiales y Oficinistas en las Oficinas Regionales

- a. En cada Oficina Regional se designará un supervisor para que en caso de ser necesario pueda cambiar los roles de los usuarios en la aplicación ACAA 21. Estos cambios serán según las necesidades del servicio. Para esto se regirán por el siguiente proceso:
 - i. El DOR deberá autorizar al supervisor el cambio a realizarse.
 - ii. El supervisor procederá a realizar el cambio.
 - iii. El supervisor preparará una bitácora de cambios en la anotará la siguiente información en cada cambio que realice:
 - A. Nombre y apellidos del usuario

- B. Nombre del usuario en el sistema (“username”)
- C. Fecha y hora en que se realiza el cambio
- D. Tipo de cambio (de oficinista a oficial o viceversa)
- E. Fecha y hora en que se revierte el cambio
- F. Firma del supervisor que realiza el cambio

8. Roles del Administrador de Redes

- a. El Administrador de Redes tiene las funciones de la administración y manejo de los equipos y aplicaciones de la red cibernética de la ACAA. Para poder ejercer todas sus funciones este requiere tener unos privilegios y accesos especiales. Sus funciones comprenden toda el área técnica de la red y todas aquellas tareas relacionadas con brindar apoyo a los usuarios de la red, la coordinación efectiva de los recursos de la red, la utilización de los archivos de los sistemas y la seguridad y el control de los accesos.
- b. El DEA de la Directoria de Informática autorizará, mediante un comunicado escrito a los Administradores de la Red a interconectarse de forma local o remota y a tener acceso a las siguientes cuentas:
 - i. Cuenta de Administrador de Dominio
 - ii. Cuenta de Administrador de Servicio
 - iii. Acceso de mantenimiento a servidores de correo electrónico
 - iv. Acceso de mantenimiento de servidores de Internet
 - v. Acceso ilimitado para creación de usuarios
 - vi. Acceso de administración de servidores para
 - A. Montar parcho de seguridad
 - B. Copiar documentos
 - C. Instalar aplicaciones
 - D. Instalar equipo de la red

E. Accesos al sistema de seguridad de entradas y salidas (puertas físicas de la Directoria)

9. Rol del Administrador de la Base de Datos

- a. El Administrador de la Base de Datos tendrá las funciones de administrar todas las bases de datos de los sistemas de la Agencia. Para poder ejercer sus funciones estos requieren tener unos privilegios y accesos especiales. Sus funciones comprenden brindar apoyo a los usuarios, la coordinación efectiva de los datos y las aplicaciones, trabajar con la aplicación que maneja el flujo del trabajo (“workflow”) y la utilización de los archivos de los sistemas.

10. Acceso Remoto a los Sistemas

- a. El DEA de la Directoria de Informática autorizará mediante comunicado escrito al administrador de la Red, a los consultores u oro proveedor de servicios a interconectarse de forma local o remota a las redes de información de la Agencia y a tener acceso a sistemas específicos para ver el comportamiento del sistema y diagnosticar posibles fallas o situaciones. Se mantendrá una bitácora de Registro del Personal con acceso remoto incluyendo en ésta la siguiente información:
 - i. Nombre de la personal con acceso remoto
 - ii. Uso dado al acceso
 - iii. Fecha desde y hasta cuando tiene el acceso

Enmiendas al Procedimiento –

Este procedimiento sólo podrá ser enmendado por el Director Ejecutivo de la Administración de Compensaciones por Accidentes de Automóviles, para atemperarlo a cambios en las leyes, o la tecnología, o como resultado de recomendaciones de los auditores internos o externos.

Vigencia

Este procedimiento será efectivo treinta (30) días a partir de su aprobación.