



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTEL GENERAL DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



HON. ANÍBAL ACEVEDO VILÁ
GOBERNADOR

(787) 289-1400

30 de octubre de 2008

Sr. Manuel Díaz Saldaña

Contralor de Puerto Rico
Oficina del Contralor
P. O. Box 366069
San Juan, Puerto Rico 00936

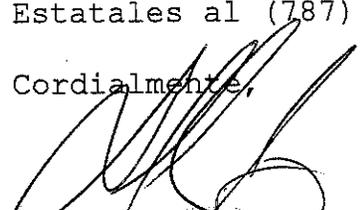
Estimado señor Díaz:

Le incluyo el Plan de Acción Correctiva (OC-DA-81) correspondiente al Informe de Auditoría DA-09-03, de la Guardia Nacional de Puerto Rico.

Con la implementación del Plan de Acción Correctiva tomaremos las medidas necesarias para corregir las deficiencias señaladas. Le daremos el seguimiento planificado de acuerdo a las normas y los Reglamentos aplicables.

Cualquier información adicional, puede solicitarla al Sr. Carmelo Crespo Cabán, Oficial Ejecutivo para Asuntos Estatales al (787) 721-3131, extensión 7001.

Cordialmente,


David Carrión Baralt

General de División, (PR), GNPR
Ayudante General

Anejos



PLAN DE ACCIÓN CORRECTIVA

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

Entidad Núm: 043

Informe de Auditoría Núm: 12678

Fecha: 22 de septiembre de 2008

Funcionario principal: GEN. DAVID CARRION BARALT

Periodo auditado: 1 de julio

de 1999 al 30 de junio de 2006

Funcionario designado: CARMELO CRESPO CABAN

Puesto: ASUNTOS ESTATALES

Teléfono: (787) 721-3131 Ext. 7000

Indique: PAC ICP

Fecha de vencimiento: 31 DE OCTUBRE DE 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>1. Promulgar normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional (Hallazgo 1-a.1) y para la administración, la seguridad y el uso de los sistemas computarizados (Hallazgo 5-a.1).</p>	<p>Con el propósito de establecer procedimientos por escrito para regir la contabilidad de la Guardia Nacional se otorgó un Contrato de Servicios Profesionales a la Compañía MASS Accounting, quien nos ofrecerá los siguientes servicios; Asistir a la Guardia Nacional en la operación del Programa <i>MIP Fund Accounting</i>, el desarrollo de un Manual de Procedimientos de Contabilidad y la implementación del Sistema de Reguisiones Electrónicas y Ordenes de Compras <i>Microix</i>. Para la administración, la seguridad y el uso de los sistemas computarizados se estableció por escrito las normas y procedimientos, la cual está en evaluación por la División Legal.</p>	<p>Parcialmente Cumplimentadas Cuando tengamos los resultados y las recomendaciones podemos establecer los manuales, las normas y procedimientos para tener sistemas seguros en todas las área.</p>

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA

Firma: (Funcionario Principal)

Fecha



PLAN DE ACCIÓN CORRECTIVA (Continuación)

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>2. Tomar las medidas necesarias para que se cumplan con las disposiciones de la Ley aplicables a los <i>Single Audits</i> y que no se repitan las situaciones comentadas en el Hallazgo 2.</p>	<p>Para evitar repetir las situaciones mencionadas en el Hallazgo 2. El 21 de noviembre de 2005 se otorgo un contrato a la firma de Auditores de la Compañía PKF, L.L.P., para que se realizaran los "<i>Single Audit</i>" de los años fiscales 2005, 2006 y 2007 de manera que nos permita cumplir con las fechas establecidas por ley y rendir los mismos a las autoridades federales (Ver Anejo 1) e impedir que vuelva ocurrir dicho Hallazgo.</p>	<p>Cumplimentado</p>

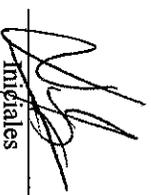

Iniciales



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

PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>3. Ver que se atiendan las recomendaciones de los informes de los <i>Single Audits</i> de los años fiscales 1999-00 al 2002-03 y años siguientes. (Hallazgos 3-a.</p>	<p>Con la intención de atender las recomendaciones de los informes de los <i>Single Audit</i>, se estableció un contrato de evaluación de Riesgos con la Compañía del CPA López Vega, quien estará evaluando el Área de la Propiedad, del Oficial Pagador Especial y el Área de Nominas, y se establecerá por escrito los diferentes procesos de las Áreas de Finanzas, Recursos Humanos y Servicios Generales. Además, se contrato a la Compañía de <i>CPA Mass Accounting</i>, los cuales asistirán a la Guardia Nacional en la Operación del Programa <i>MIP Fund Accounting</i> (Sistema de Contabilidad de la Agencia), desarrollarán un Manual de Procedimientos de Contabilidad cual servirá de herramienta en la operación del Sistema de Contabilidad en la Agencia. Con dichos servicios se logrará que la contabilidad refleje balances confiables, se establecerán controles adecuadas para salvaguardar los activos y se realizara las conciliaciones en forma eficiente. Esta acción traerá la corrección de los diferentes hallazgos y evitará que los mismos se repitan.</p>	<p>Parcialmente cumplimentado</p>


Iniciales



PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>4. Ver el Comité de Ética de la Guardia Nacional y el Oficial Ejecutivo para Asuntos Estatales cumplan con sus responsabilidades de velar porque se cumplan las recomendaciones de los Informes de los <i>Single Audits</i>. (Hallazgo 3-a-2)</p>	<p>Además, estamos en proceso de comprar del módulo del Registro de la Propiedad del Sistema MIP, el cual estará ingresado en el módulo de nuestro Sistema de Contabilidad y en adición contiene toda la información relacionada con el equipo de la propiedad incluyendo sus codificaciones.</p> <p>Con estas medidas los hallazgos serán corregidos y no se repetirán.</p> <p>Anteriormente el Comité de Ética no recibía los resultados de las diferentes auditorías, no obstante, el reciente nombrado Oficial Ejecutivo para Asuntos Estatales estableció que dichos informes le serán entregados al Comité de Ética para la acción que corresponda. Recientemente, se reestructuro también el Comité de Ética de la Agencia.</p>	<p>Parcialmente cumplimentado</p> <p>Entendemos que dichos cambios cumplirán con las necesidades que enfrenta nuestra Agencia y los hallazgos serán corregidos para una sana administración.</p>


Iniciales



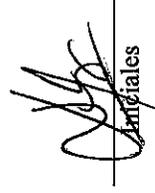
PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>c) Realicen análisis de las facturas al cobro cuyas gestiones de cobro resulten infructuosas y se refieran al Departamento de Hacienda o al Secretario de Justicia, según corresponda. (Hallazgo 4-a.2)</p> <p>2. La Directora Auxiliar de Finanzas y comprobantes de pago correspondientes a los fondos de mejoras permanentes en el sistema de contabilidad mecanizado MIP y que no se repitan situaciones como la comentada en el Hallazgo 1-a.3.</p> <p>b. El Oficial Principal de Informática:</p> <p>1) Mantenga los respaldos de la información almacenada en los medios electrónicos en un lugar seguro fuera de los predios de la agencia. (Hallazgo 5-a.2)</p>	<p>Una vez se completen los adiestramientos y se Finalice el manual de procedimientos, se incorporarán medidas de controles para anticipar cualquier deficiencia y corregirla. Se mantendrá una continúa supervisión para asegurarnos que los procedimientos se realicen.</p> <p>El Contador I, a cargo de entrar las facturas al cobro al Sistema MIP, emitirá un informe detallado, de manera que se evalué si las mismas se referirán al Departamento de Justicia o al Departamento de Hacienda, según sea el caso.</p> <p>Actualmente la Directora Auxiliar de Finanzas y Presupuestos mantiene sus registros y conciliaciones de las Mejoras Permanentes debidamente actualizado.</p> <p>Referente a los respaldos de la información almacenada en medios electrónicos, le informo que según certificación emitida por el Coronel Retirado Ramón L. Díaz Santiago, Oficial Administrativo del Comando, de la Guardia Nacional los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto corregido dicho hallazgo.</p>	<p><i>[Signature]</i> Jefes</p>



PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>2) Preparar, para la aprobación del Ayudante General, un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. (Hallazgo 5-a.3).</p>	<p>Rico se mantienen almacenados bajo llave en la ubicada en Isla Grande, fuera de los predios de nuestra Agencia. Por tal razón, damos por corregido dicho hallazgo. (Ver Anejo 2)</p> <p>Con relación a la implementación del Plan de Contingencia, se hicieron las coordinaciones pertinentes. No obstante, actualmente no contamos con el presupuesto necesario para su implementación.</p> <p>Estamos realizando las gestiones necesarias para identificar fondos para ese propósito.</p>	


Comptroller

Diaz Anibal (Oficina de Tecnologia e Información)

From: Garcia, Gustavo SSG [g.garciamorales@us.army.mil]
Sent: Wednesday, April 09, 2008 4:04 PM
To: Jeffrey Rouille Figna; Diaz Anibal (Oficina de Tecnologia e Información)
Cc: Couverthie, Manuel CW2; Ortiz, Jose CW3; Rodriguez, Carlos A. LTC; Crespo, Luis G. SGT
Subject: Tape Drive Upgrade Recommendations
Signed By: There are problems with the signature. Click the signature button for details.

Good afternoon,

As we all know, as part of the Disaster Recovery solution, all Tape medias must be on the same standard/format which is LTO. In order for this step to be accomplished, GNPR and FIGNA will have to upgrade their Tape Drives to support LTO formats. Based on what I saw, your ISA servers have SCSI cards and can support external Tape Drives. Refer below for recommendations:

Dell: http://www.dell.com/content/products/productdetails.aspx/pvaul_110tito3?c=us&cs=04&l=en&s=bsd

Compaq: <http://www.provantage.com/hp-compaq-q1539b-aba~7HEWS36C.htm>


24/04/08
G. Garcia



Data Supplies

ORIGINAL - CUSTOMER

CORPORATION
Villa Nevárez Commercial Center • Río Piedras
Tel. (787) 758-7118 • Fax (787) 250-0028
REMIT TO: PO Box 41147 San Juan, PR 00940-1147

06/02/08	309918
DATE	NUMBER

INVOICE

INKS • TONERS • RIBBONS • PAPER • LABELS

SOLD TO: FIDEICOMISO GDA. NACIONAL

SHIP TO: PDA 3 1/2 PTA DE TIERRA
ATN: ANA LUGO
TEL. 289-1440

7700A ROAD SUITE 303 WOODR

ORDER NO.	ORDER DATE	CUST. NO.	SHIP VIA	SHIP DATE	TERMS
151793	06/02/08	FIGNAC DAN	OUR TRUCK	05/13/08	CASH ON DELIVE

QUANTITY ORDERED	UNIT	QTY. SHIPPED	ITEM NUMBER	ITEM DESCRIPTION	UNIT	UNIT PRICE	EXTENDED AMOUNT
2	EA	2	*	HP STORAGE WORKS ULTRIUM 960 TAPE DRIVE LTD Q1539B	EA	3,249.00	6,498.00
22	EA	22	*	HP LTD ULTRIUM 3 400/800 TAPE C7973A	EA	49.95	1,098.90

Dejar validos y certificar - Credito PO - Refund: verificar factura 6/14/08 y preparar cheque - ¿Cajero?

Nota para de validad absoluta, certifico que ningún servidor público del Fed. Guardia Nacional es parte o tiene algún interés en las ganancias o beneficios producto del contrato objeto de esta factura y de ser parte o tener interés en las ganancias o beneficios producto del contrato ha mediado una dispensa previa. La única consideración para suministrar los bienes o servicios objeto del contrato ha sido el pago acordado con el representante autorizado de la Agencia.

El importe de esta factura es justo y correcto. Los trabajos de construcción han sido realizados, los productos han sido entregados o los servicios prestados y no han sido pagados*

Juan L.

CERTIFICADO CORRECTO

10 JUN 2008

PRG 02071524 \$7,596.90

IMPORTANT: THIS IS YOUR INVOICE. NO OTHER INVOICE WILL BE SENT PLEASE APPROVE AND FORWARD TO ACCOUNTS PAYABLE FOR PAYMENT

We certify that the above invoice is true and correct and that payment thereof has not been received.	SALE AMOUNT	7,596.90
	INVOICE TOTAL	7,596.90

Received in Good Condition: _____

By: _____ Date: _____

We reserve the right to charge the maximur interest rate permitted by law on all past du invoices.

FIGNA

PO BOX 9023786
SAN JUAN, PUERTO RICO 00902-3786
(787)289-1420 fax (787)721-1836

Purchase Order No. 2008-153

Transmittal in person
14 May 08

PURCHASE ORDER

Vendor

Name	DATA SUPPLY
Address	
City	PR
Phone	787-758-7118

Ship To

Name	FIGNA
Address	P O BOX 9023786
City	SAN JUAN PR 00902-3786
Phone	787-289-1420

Qty	Units	Description	Unit Price	TOTAL
2	1	DOIM HP STORAGE WORKS ULTRIUM 960 TAPE DRIVE LTO ULTRIUM (400 GB/800GB) ULTRIUM 3 SCSI LVS EXTERNAL Q1539B THIS ITEM HAS A 3 YEARS WARRANTY PROVIDED BY THE MANUFACTURER	\$3,249.00	\$6,498.00
22	2	HP-LTO ULTRIUM 3 400GB/800GB-GOLD- STORAGE MEDIA C7973A	\$49.95	\$1,098.90
			SubTotal	\$7,596.90
			Shipping & Handling State	
			TOTAL	\$7,596.90

AW
5/15/08

5 MAYO 2008

[Signature]



COMMONWEALTH OF PUERTO RICO
PUERTO RICO NATIONAL GUARD
JOINT FORCES HEADQUARTERS
THE ADJUTANT GENERAL'S OFFICE
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



HON. ANÍBAL ACEVEDO VILÁ
GOVERNOR

(787) 289-1400

PRSG-CAO

14 de Agosto de 2008

CERTIFICACION

Por la siguiente certifico que, los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto Rico, se mantienen Almacenados bajo llave en la oficina de la Guardia Estatal de Puerto Rico. Estos "Back up Tapes" son removidos por el oficial autorizado/encargado del área de Informática, Sr. Anibal Díaz, desde el 12 de enero de 2008, cuando el Programador oficial de la Guardia Nacional de Puerto Rico Sr. Nelson Reyes renunció.

Atentamente,


Ramon L. Díaz-Santiago
Col (RET) EEU
Oficial Administrativo del Comando
Guardia Estatal


R-
Anibal Díaz



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTEL GENERAL DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



HON. LUIS G. FORTUÑO BURSET
GOBERNADOR

(787) 289-1400

26 de febrero de 2009

Sr. Manuel Díaz Saldaña
Contralor de Puerto Rico
Oficina del Contralor
P. O. Box 366069
San Juan, Puerto Rico 00936

Estimado señor Díaz:

Le incluyo el segundo informe complementario del Plan de Acción Correctiva (OC-DA-81), correspondiente al Informe de Auditoría DA-09-03, de la Guardia Nacional de Puerto Rico.

Hemos implementado el Plan de Acción Correctiva y tomaremos las medidas necesarias para corregir las deficiencias señaladas. Continuaremos con el seguimiento planificado de acuerdo a las normas y los Reglamentos aplicables.

Cualquier información adicional, puede solicitarla al Sr. Víctor M. Ortiz, Oficial Ejecutivo para Asuntos Estatales al (787) 721-3131, extensión 7001.

Cordialmente,


Antonio J. Vicéns
General de Brigada (Ret), GNPR
Ayudante General

Anejos



PLAN DE ACCIÓN CORRECTIVA

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

Entidad Núm: 043

Informe de Auditoría Núm: 12678

Fecha: 26 de febrero de 2009

Funcionario principal: GEN. ANTONIO J. VICENS

Período auditado: 1 de julio

de 1999 al 30 de junio de 2006

Funcionario designado: VICTOR M. ORTIZ

OFICIAL EJECUTIVO PARA ASUNTOS ESTATALES

Teléfono: (787) 721-3131 Ext. 7000

Indique: PAC ICP-1

Fecha de vencimiento: 1RO MARZO 2009

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>1. Promulgar normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional (Hallazgo 1-a.1) para la administración, la seguridad y el uso de los sistemas computarizados (Hallazgo 5-a.1).</p>	<p>Con el propósito de establecer procedimientos por escrito para regir la contabilidad de la Guardia Nacional de otorgó un Contrato de Servicios Profesionales a la Compañía MASS Accounting, quien nos ofrecerá los siguientes servicios; Asistir a la Guardia Nacional en la operación del Programa <i>MIP Fund Accounting</i>, el desarrollo de un Manual de Procedimientos de Contabilidad y la Implementación del Sistema de Requisiciones Electrónicas y Ordenes de Compras <i>Microix</i>. Para la administración, la seguridad y el uso de los sistemas computarizados se estableció por escrito las normas y procedimientos, y esta en evaluación por la División Legal.</p>	<p>Parcialmente Cumplimentadas. Debido a los cambios de administración, aún estamos en el proceso de los nombramientos de los nuevos Ejecutivos de Agencia. A esos efectos, el proceso de auditorías y servicios profesionales se encuentran parcialmente detenidos, hasta tanto se nombren todos los puestos de confianza de la Agencia, incluyendo el abogado del área estatal y el Oficial de Informática, etc. Estamos en espera de la aprobación de OGP para dichos nombramientos. Estamos en proceso en darle continuidad para terminar de estos contratos. Tan pronto tengamos los resultados, evaluaciones y todas las recomendaciones estableceremos los manuales, las normas y los procedimientos para garantizar un sistema seguro en todas las áreas.</p>

(Véase instrucciones al dorso)

CERTIFICO QUE ESTA INFORMACION ES CORRECTA

ANTONIO J. VICENS
General de Brigada (Ret), GNPRI, Ayudante General
Firma (Funcionario Principal)

26 FEB 09
Fecha



Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>2. Tomar las medidas necesarias para que se cumplan con las disposiciones de las Leyes Aplicables a los <i>single audits</i> y que no se repitan las situaciones comentadas.</p>	<p>Hemos establecido un Contrato de Servicios Profesionales con el CPA López, Vega quien realizará una evaluación de riesgos y de los procesos de la Guardia Nacional. Dicho contrato nos servirá de herramienta para establecer los procedimientos por escritos de manera que las situaciones comentadas en los <i>single audits</i> sean corregidos para garantizar que las mismas no se repitan.</p>	<p>Parcialmente Cumplimentado. Se orientó al Director de Servicios Generales, para que se otorguen los contratos dentro del tiempo reglamentario, de manera que se cumpla con la fecha límite del informe final evitando el hallazgo mencionado.</p>
<p>3. Ver que se atiendan las recomendaciones de los informes de los <i>single audits</i> de los años fiscales 1999-00 al 2002-03 y años siguientes (Hallazgos 3-a.1)</p>	<p>Se estableció un Contrato de Evaluación de Riesgos con la Compañía del CPA López, Vega, quien estará evaluando el Área de la Propiedad, al Oficial Pagador Especial y el Área de Nóminas. Con el manual de procedimiento se tomarán las medidas correctivas de una forma eficiente y rápida. Además, estableceremos por escrito todos los procesos de las diferentes áreas, Finanzas, Recursos Humanos y Servicios Generales. Con este sistema se corregirán los diferentes hallazgos y evitaremos que los mismos se repitan.</p>	<p>Parcialmente Cumplimentado. Estamos en el proceso de la culminación de los contratos mencionados para desarrollar el Manual de Contabilidad de la Política y Procesos; el Registro de Propiedad y evitar la falta de confiabilidad de las entradas de jornal para que el balance inicial de efectivo sea el correcto para el próximo año fiscal. El cambio de personal ha retrasado la culminación de estos trabajos.</p>

[Signature]

Iniciales

OC-DA-81



RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>4. Ver que el Comité de Ética de la Guardia Nacional y el Oficial Ejecutivo para Asuntos Estatales cumplan con sus responsabilidades de velar porque se atiendan las recomendaciones de los informes de los <i>single audits</i>.</p>	<p>Como medidas de acción se han efectuado cambios en el personal de la Guardia Nacional. Se nombró un nuevo Oficial Ejecutivo para Asuntos Estatales y una nueva Directora de Finanzas y Presupuestos. Anteriormente el Comité de Ética no recibía los resultados de las diferentes auditorías, no obstante, el Oficial Ejecutivo para Asuntos Estatales estableció que dichos informes se entregarán al Comité de Ética para la acción que correspondan. También velará para que se cumplan con las recomendaciones de los informes de <i>Single Audits</i>. La Directora de Finanzas y Presupuesto recomendó establecer un contrato con la compañía <i>MAAS Accounting</i>, el cual asistirá a la Guardia Nacional en la Operación del Programa <i>MIP Fund Accounting</i> (Sistema de Contabilidad de la Agencia), se implementará un Manual de Procedimientos de Contabilidad el cual servirá de herramienta en la operación del Sistema de Contabilidad en la Agencia. También, se estableció un Contrato de Servicios Profesionales con el CPA López Vega, quien evaluará los diferentes procesos y riesgos, los cuales cubrirán las áreas afectadas. Entendemos que con dichos cambios cumpliremos con las necesidades que enfrenta nuestra Agencia y corregiremos los hallazgos.</p>	<p>Parcialmente Cumplimentado. Actualmente estamos en el proceso de crear de un nuevo Comité de Ética en la Agencia. Tan pronto el mismo se establezca se le entregará copia de los resultados de las auditorías para que cumplan con las recomendaciones de los hallazgos.</p>

ASU
 Iniciales
 OC-DA-81



RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>5. Ver que el Oficial Ejecutivo para Asuntos Estatales cumpla con su responsabilidad y ejerza una supervisión eficaz del personal, y se asegure de que:</p> <p>a) El Director de Finanzas y Presupuesto cumpla con las disposiciones de ley y los reglamentos, las normas de sana administración, el control interno y se asegure de que:</p> <p>1. Los contadores:</p> <p>a) Consoliden todos los datos financieros en el sistema <i>Micro Information Product (MIP)</i>, de manera que se pueda ofrecer información financiera confiable.</p> <p>b) Mantengan un registro de las cuentas por cobrar en el Módulo del Mayor General del Sistema MIP que incluya, entre otras cosas, el número de objeto, nombre del proveedor, fecha de la factura al cobro emitida, y que realicen análisis de dichas cuentas de acuerdo con la fecha de vencimiento. (Hallazgo 1-a.4)</p>	<p>Efectivo el 5 de febrero de 2008, la Oficina de Gerencia y Presupuesto nos autorizó a cubrir el puesto de Oficial Ejecutivo para Asuntos Estatales. Dicho funcionario ha realizado las gestiones pertinentes para una supervisión efectiva, para corregir las diferentes deficiencias en el Área de Finanzas y Presupuestos. Estas incluyen utilizar el Sistema de Contabilidad <i>MIP</i> en su mayor capacidad.</p> <p>Para lograrlo se estableció un Contrato con la Compañía <i>MASS Accounting</i>, quienes orientan y adiestran a los Contadores de la Oficina de Finanzas, para que utilicen el Sistema MIP uniformemente y que se corrija la información financiera suministrada.</p> <p>Además, estamos realizando las entradas al Sistema MIP de las Facturas al Cobro y se harán las gestiones de cobro de manera efectiva, según el Reglamento Num. 44 "Deudas no Contributivas Existentes a Favor del Gobierno de Puerto Rico".</p>	<p>RESULTADO</p> <p>Continúa Parcialmente Cumplimentado. Estamos en proceso de la culminación de los contratos antes mencionados, de manera que alcancemos una contabilidad confiable y se corrija la información financiera suministrada. También, se comenzó a evaluar las Hojas de Deberes de los Contadores de manera que las mismas estén acorde con la realidad actual de la Agencia y con las responsabilidades de los funcionarios.</p> <p>Parcialmente cumplimentado se implementará un Manual de Procedimientos de Contabilidad el cual servirá de guía en la operación del Sistema de Contabilidad en la Agencia. Se estableció un Contrato de Servicios Profesionales con el CPA López Vega, para evaluar los diferentes procesos y riesgos en todas las áreas.</p> <p>Parcialmente cumplimentado las Facturas al Cobro se están registrando en el Sistema de MIP y se realizan las gestiones de cobro, según lo establece el Reglamento 44, para esos fines.</p>

ASL

Iniciales

OC-DA-81



RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>c) Realicen gestiones de cobro efectivas, dentro del término requerido para ello, y se utilice el formulario correspondiente (Hallazgo 4-a.1)</p> <p>d) Realicen análisis de las facturas al cobro cuyas gestiones de cobro resulten infructuosas y se refieran al Departamento de Hacienda o al Secretario de Justicia, según corresponda. (Hallazgo 4-a.2)</p>	<p>Cuando el Contador reciba las Facturas al Cobro se entrarán al Sistema MIP, y se realizarán las gestiones de cobro dentro del término requerido de acuerdo a la Reglamentación Núm. 44.</p> <p>El Contador I, a cargo de entrar las facturas al cobro al Sistema MIP, emitirá un informe detallado, para evaluar si las mismas se referirán al Departamento de Justicia o al Departamento de Hacienda, según sea el caso.</p> <p>Actualmente la Directora Auxiliar de Finanzas y Presupuesto mantiene sus registros y las conciliaciones de las Mejoras Permanentes debidamente actualizado.</p>	<p>Parcialmente cumplimentado estamos realizando las entradas al Sistema MIP de las Facturas al Cobro y se harán las gestiones de cobro de manera efectiva, según el Reglamento Num. 44.</p> <p>Parcialmente cumplimentado se evaluarán todas las Facturas al Cobro y cuando las gestiones de cobro sean infructuosas se referirán al Departamento de Justicia o al Departamento de Hacienda, según sea el caso.</p> <p>Parcialmente cumplimentado según la comunicación recibida el 26 de noviembre de 2008, su oficina le dará seguimiento a los registros y conciliaciones de las mejoras Permanentes, no obstante, la Directora Auxiliar de Finanzas y Presupuesto fue instruida a que mantenga los registros de contabilidad de las mismas debidamente actualizada.</p>
<p>2. La Directora Auxiliar de Finanzas y Presupuesto registre con prontitud los comprobantes de pago correspondientes a los fondos de Mejoras Permanentes en e Sistema de Contabilidad mecanizado MIP y que no se repitan situaciones como la comentada en el Hallazgo 1-a.3.</p>		

ASL

Initiales

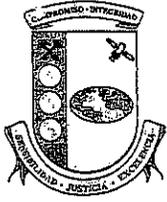


RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>a. El Oficial Principal de Informática:</p> <p>1) Mantenga los respaldos de la información almacenada en los medios electrónicos en un lugar seguro fuera de los predios de la Agencia. (Hallazgo 5-a.2)</p> <p>2) Prepare, para la aprobación del Ayudante General, un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. (Hallazgo 5-a.3).</p>	<p>Referente a la información almacenada en medios electrónicos, le informo que según certificación emitida por el Coronel Retirado Ramón L. Díaz Santiago, Oficial Administrativo del Comando, de la Guardia Nacional los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto Rico se mantienen almacenados bajo llave en la Oficina de la Guardia Estatal, esta oficina quedan ubicada en la Base de Isla Grande, fuera de los predios de nuestra Agencia. Por tal razón, damos por corregido dicho hallazgo.</p> <p>Con relación a la implementación del Plan de Contingencia, se realizaron las coordinaciones pertinentes para establecer el mismo. Actualmente no contamos con el presupuesto para implementarlo. No obstante, estamos realizando las gestiones necesarias de identificar fondos para ese propósito.</p>	<p>Cumplimentado con relación a el hallazgo de los <i>Back up</i> de la Oficina de Informática, este fue corregido, según comunicación recibida de sus oficinas el 26 de noviembre de 2008.</p> <p>Parcialmente cumplimentado el desarrollo de un Plan de Contingencia aún se encuentra en proceso, hasta tanto la Oficina de Gerencia y Presupuesto autorice cubrir la posición de Oficial de Informática, ya que hemos identificado fondos para ese propósito. Además, de la creación del Manual de Procedimientos Internos de esa Oficina.</p>

ASL

Iniciales

OC-DA-81



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

DIVISION SERVICIOS
ADMINISTRATIVOS
RECIBIDO

2008 DEC -8 PM 4:02

26 de noviembre de 2008

Col. David Baralt Carrión
Ayudante General
Guardia Nacional de Puerto Rico
San Juan, Puerto Rico

Estimado coronel Baralt Carrión:

Evaluamos el **Plan de Acción Correctiva (PAC)** que nos sometió para el **Informe de Auditoría DA-09-03** de la Guardia Nacional de Puerto Rico (Guardia Nacional). Determinamos que la **Recomendación 5.b.1)** se considera cumplimentada, las **1, 2, 4 y 5.a.1)d)** y **5.b.2)** parcialmente cumplimentadas y de la **5.a.1)a) a la c.)** no cumplimentada. A las recomendaciones **3 y 5.a.2)** no le daremos seguimiento. Las medidas tomadas para cumplimentar éstas últimas se verificarán en la próxima auditoría.

Agradeceremos que en el **Informe Complementario al Plan de Acción Correctiva (ICP-1)** nos suministre la siguiente información y documentos:

1. Evidencia de haberse promulgado normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional [**Hallazgo 1-a.1)**] y para la administración, la seguridad y el uso de los sistemas computadorizados [**Hallazgo 5-a.1)**]. [**Recomendación 1)**]
2. Informar si de acuerdo a las medidas tomadas se cumple con las disposiciones de la ley aplicables a los *single audits*. [**Recomendación 2)**]
3. Medidas tomadas para asegurarse que el Comité de Ética de la Guardia Nacional y el Oficial Ejecutivo para Asuntos Estatales cumplan con sus responsabilidades de velar porque se atiendan las recomendaciones de los informes de los *single audits*. [**Recomendación 4)**]
4. Medidas tomadas para ver que el Oficial Ejecutivo para Asuntos Estatales cumpla con su responsabilidad y ejerza una supervisión eficaz del personal, y se asegure de que:
 - a. El Director de Finanzas y Presupuesto cumpla con las disposiciones de ley y reglamento, y normas de sana administración y de control interno y se asegure de que:
 - 1) Los contadores:
 - a. Consoliden todos los datos financieros en el Sistema *Micro Information Product (MIP)*, de manera que se pueda ofrecer información financiera confiable. [**Recomendación 5.a.1)a)**]

Rosa de Francisco Díaz 08/10/08
Araaldo Francisco López 8/6/08
Blades - 6/ julio/08.
Amalio Amador 6/ julio/08
Alfonso Ruiz 6/ julio/08
Alfonso
11/ agosto/08

Stearns M. Mejía
Comité de Ética
12/ agosto/2008

INFORME DE AUDITORÍA DA-09-03
18 de julio de 2008
GUARDIA NACIONAL DE PUERTO RICO
(Unidad 1422 - Auditoría 12678)

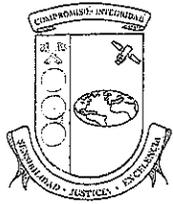
Período auditado: 1 de julio de 1999 al 30 de junio de 2006

CONTENIDO

	Página
INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
RESPONSABILIDAD DE LA GERENCIA	5
ALCANCE Y METODOLOGÍA	5
OPINIÓN.....	6
RECOMENDACIONES	6
AL AYUDANTE GENERAL	6
CARTAS A LA GERENCIA.....	8
COMENTARIOS DE LA GERENCIA.....	8
AGRADECIMIENTO	9
RELACIÓN DETALLADA DE HALLAZGOS.....	10
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	10
HALLAZGOS EN LA GUARDIA NACIONAL	11
1 - Ausencia de normas y procedimientos escritos para regir las operaciones de contabilidad en la Oficina de Finanzas y Presupuesto, sistemas de contabilidad utilizados sin consolidar la base de datos financieros, comprobantes no registrados en el sistema de contabilidad mecanizado y ausencia de información de las cuentas por cobrar	11
2 - Incumplimiento de disposiciones relacionadas con las auditorías integradas (<i>single audits</i>) de los estados financieros y con la radicación de los informes de situación financiera a las autoridades federales.....	16
3 - Incumplimiento de las recomendaciones contenidas en los informes de los <i>single audits</i> rendidos por la sociedad de contadores públicos autorizados	21
4 - Gestiones de cobro inefectivas y otra deficiencia relacionada con las facturas al cobro.....	24

5 - Ausencia de normas y procedimientos escritos para regir las operaciones
relacionadas con los sistemas de información computadorizado y otras fallas
de control relacionadas27

**ANEJO - FUNCIONARIOS Y EMPLEADOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO34**



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

DIVISION DE SERVICIOS
ADMINISTRATIVOS
RECIBIDO

2009 APR -3 PM 8:46

27 de marzo de 2009

Gen. Antonio J. Vicens González
Ayudante General
Guardia Nacional
San Juan, Puerto Rico

Estimado general Vicens González:

Evaluamos el **Informe Complementario al Plan de Acción Correctiva (ICP-1)** que nos sometió para el **Informe de Auditoría DA-09-03** de la Guardia Nacional de Puerto Rico (Guardia Nacional). Determinamos que las **recomendaciones 1, 2 y de la 5.a.1)a a la c) y b.2)** se consideran parcialmente cumplimentadas. A las **recomendaciones 4 y 5.a.1)d)** no le daremos seguimiento. Las medidas tomadas para cumplimentar éstas últimas se verificarán en la próxima auditoría.

Agradeceremos que en el **Informe Complementario al Plan de Acción Correctiva (ICP-2)** nos suministre la siguiente información y documentos:

1. Evidencia de haberse promulgado normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional [**Hallazgo 1-a.1)**] y para la administración, la seguridad y el uso de los sistemas computadorizados [**Hallazgo 5-a.1)**]. [**Recomendación 1)**]
2. Informar si de acuerdo a las medidas tomadas se cumple con las disposiciones de la ley aplicables a los *single audits*. [**Recomendación 2)**]
3. Medidas tomadas para ver que el Oficial Ejecutivo para Asuntos Estatales cumpla con su responsabilidad y ejerza una supervisión eficaz del personal, y se asegure de que:
 - a. El Director de Finanzas y Presupuesto cumpla con las disposiciones de ley y reglamento, y normas de sana administración y de control interno y se asegure de que:
 - 1) Los contadores:
 - a. Consoliden todos los datos financieros en el Sistema *Micro Information Product (MIP)*, de manera que se pueda ofrecer información financiera confiable. [**Recomendación 5.a.1)a)**]
 - b. Mantengan un registro de las cuentas por cobrar en el Módulo del Mayor General del Sistema *MIP* que incluya, entre otras cosas, el número de objeto, el nombre del proveedor y la fecha de la factura al cobro emitida, y realicen análisis de dichas cuentas de acuerdo con la fecha de vencimiento. [**Recomendación 5.a.1)b)**]
 - c. Realicen gestiones de cobro efectivas, dentro del término requerido para ello, y utilicen el formulario correspondiente. [**Recomendación 5.a.1)c)**]



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTELES GENERALES DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



Hon. Luis G. Fortuño Bursset
Gobernador

(787) 289-1400

4 de septiembre de 2009

Sr. Manuel Díaz Saldaña

Contralor de Puerto Rico
Oficina del Contralor
P. O. Box 366069
San Juan, Puerto Rico 00936

Estimado señor Díaz:

Le incluyo el Plan de Acción Correctiva (OC-DA-81), correspondiente al Informe de Auditoría DA-09-03, de la Guardia Nacional de Puerto Rico.

Con la implementación del Plan de Acción Correctiva tomaremos las medidas necesarias para corregir las deficiencias señaladas. Le daremos el seguimiento planificado de acuerdo a las normas y los Reglamentos aplicables.

Cualquier información adicional, puede solicitarla al Sr. Víctor M. Ortiz, Oficial Ejecutivo para Asuntos Estatales al (787) 721-3131, extensión 7001.

Cordialmente,


Antonio J. Vicéns
General de Brigada, GNPR
Ayudante General

Anejos



PLAN DE ACCIÓN CORRECTIVA

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

Entidad Núm: 043

Informe de Auditoría Núm: DA-09-03

Fecha: 2 de septiembre de 2009

Funcionario principal: GEN. ANTONIO J. VICENS

Período auditado: 1 de julio de 1999 al 30 de junio de 2006

de 1999 al 30 de junio de 2006

Funcionario designado: VICTOR M. ORTIZ

Puesto: ASUNTOS ESTATALES

Teléfono: (787) 721-3131 Ext. 7000

Indique: PAC ICP-1

Fecha de vencimiento: 1 julio 2009

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>1. Promulgar normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional (Hallazgo 1-a.1) para la administración, la seguridad y el uso de los sistemas computarizados (Hallazgo 5-a.1).</p>	<p>Con el propósito de establecer procedimientos por escrito para regir la contabilidad de la Guardia Nacional de otorgó un Contrato de Servicios Profesionales a la Compañía MASS Accounting, quien nos ofrecerá los siguientes servicios; Asistir a la Guardia Nacional en la operación del Programa <i>MIP Fund Accounting</i>, el desarrollo de un Manual de Procedimientos de Contabilidad y la Implementación del Sistema de Requisiciones Electrónicas y Ordenes de Compras <i>Microix</i> al presente esta en evaluación por la División Legal.</p>	<p>PARCIALMENTE CUMPLIMENTADO Estamos en el proceso de evaluación del Manual de Procedimiento de Contabilidad del Sistema de Contabilidad (MIP). Adjunto el Manual para la Aprobación de Requisiciones Electrónicas en Microix (Ver Anejo 1) y el Manual de Instrucciones para Requisiciones Electrónicas Microix (Ver Anejo 2). Para la administración, la seguridad y el uso de los sistemas computarizados se estableció por escrito las normas y procedimientos, y esta en evaluación por la División Legal.</p>

(Véase instrucciones al dorso)

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA

ANTONIO J. VICENS

General de Brigada, GNPR, Ayudante General

Firma (Funcionario Principal)

1 de septiembre de 2009

Fecha



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

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>2. Tomar las medidas necesarias para que se cumplan con las disposiciones de las Leyes Aplicables a los <i>Single Audits</i> y que no se replantan las situaciones comentadas.</p>	<p>Hemos establecido el Contrato de Servicios Profesionales con el CPA López, Vega quien realizará la auditoria del "Single Audit" 2009, en la fecha señalada.</p>	<p>PARCIALMENTE CUMPLIMENTADO. Se cumplirá con la fecha límite del informe final evitando el hallazgo mencionado. (Ver Anexo 3)</p>
<p>3. Ver que el Oficial Ejecutivo para Asuntos Estatales cumpla con su responsabilidad y ejerza una supervisión eficaz del personal, y se asegure de que:</p> <p>a) El Director de Finanzas y Presupuesto cumpla con las disposiciones de ley y los reglamentos, las normas de sana administración, el control interno y se asegure de que:</p>	<p>El Oficial Ejecutivo para Asuntos Estatales ha realizado las gestiones pertinentes para una supervisión efectiva conforme a las normas y reglamentos a cabalidad.</p> <p>La Directora de Finanzas y Presupuesto velará que su área cumpla con la reglamentación vigentes, de acuerdo a la ley de acuerdo y con las normas de una de sana administración. Incluyendo utilizar el Sistema de Contabilidad <i>MIP</i> en su mayor capacidad.</p>	<p>CUMPLIMENTADO El Oficial Ejecutivo para Asuntos Estatales vigilará que se cumpla con la reglamentación y las normas de sana administración del personal que esté bajo su supervisión.</p>

ML

Iniciales

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>1. Los contadores:</p> <p>a) Consoliden todos los datos financieros en el sistema <i>Micro Information Product (MIP)</i>, de manera que se pueda ofrecer información financiera confiable. (Hallazgo 5.a.1)a)</p> <p>b) Mantengan un registro de las cuentas por cobrar en el Módulo del Mayor General del Sistema MIP que incluya, entre otras cosas, el número de objeto, nombre del proveedor, fecha de la factura al cobro emitida, y que realicen análisis de dichas cuentas de acuerdo con la fecha de vencimiento. (Hallazgo 5.a.1)b)</p>	<p>Para lograrlo se estableció un Contrato con la Compañía <i>MASS Accounting</i>, quienes orientan y adiestran a los Contadores de la Oficina de Finanzas, para que utilicen el Sistema MIP uniformemente y que se corrija la información financiera suministrada.</p> <p>Además, estamos realizando las entradas al Sistema MIP de las Facturas al Cobro y se harán las gestiones de cobro de manera efectiva, según el Reglamento Núm. 44 "Deudas no Contributivas Existentes a Favor del Gobierno de Puerto Rico".</p>	<p>PARCIALMENTE CUMPLIMENTADO.</p> <p>Estamos en la evaluación final del Manual de Procedimientos de Contabilidad el cual servirá de guía en la operación del Sistema de Contabilidad en la Agencia.</p> <p>CUMPLIMENTADO</p> <p>Las Facturas al Cobro se están registrando en el Sistema de MIP y se realizan las gestiones de cobro, según lo establece el Reglamento 44, para esos fines. (Ver anejo 4)</p>


 Iniciales
 OC-DA-81



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

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>c) Realicen gestiones de cobro efectivas, dentro del término requerido para ello, y se utilice el formulario correspondiente (Hallazgo 5.a.1)c)</p>	<p>Cuando el Contador reciba las Facturas al Cobro se entraran al Sistema MIP, y se realizarán las gestiones de cobro dentro del término requerido de acuerdo a la Reglamentación Núm. 44.</p> <p>El Contador I, a cargo de entrar las facturas al cobro al Sistema MIP y la Directora de Finanzas y Presupuesto realizan las gestiones necesarias para recobrar los referidos fondos públicos. Se analizará las facturas al cobro cuyas gestiones de cobro resulten infructuosas y se refieran al Departamento de Hacienda o al Secretario de Justicia, según corresponda.</p>	<p>CUMPLIMENTADO</p> <p>Se realizan las gestiones de cobros utilizando los formularios establecidos según el Reglamento Núm. 44. (Ver Anejo 5 y 6)</p> <p>Se realizan las gestiones necesarias para recobrar los referidos fondos públicos (Ver Anejo 7 y 8)</p>


Iniciales
OC-DA-81



RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>a. El Oficial Principal de Informática:</p> <p>Prepare, para la aprobación del Ayudante General, un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. (Hallazgo 5-a.2).</p>	<p>La información almacenada en medios electrónicos, de acuerdo a certificación emitida por el Coronel Retirado Ramón L. Díaz Santiago, Oficial Administrativo del Comando, de la Guardia Nacional los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto Rico se mantienen almacenados bajo llave en la Oficina de la Guardia Estatal, esta oficina queda ubicada en la Base de Isla Grande, fuera de los predios de nuestra Agencia</p> <p>La implementación del Plan de Contingencia, se realiza en coordinación de las recomendaciones de la auditoría de riesgos y procesos y en este momento esta en revisión de l Asesor Legal.</p>	<p>CUMPLIMENTADO</p> <p>Los <i>Back up</i> de la Oficina de Informática, se mantienen almacenados bajo llave en la Oficina de la Guardia Estatal, en la Base de Isla Grande, fuera de nuestra Agencia</p> <p>PARCIALMENTE CUMPLIMENTADO</p> <p>El Plan de Contingencia aún se encuentra en proceso de evaluación, tan pronto se tenga el Manual de Procedimientos Internos de esta Oficina.</p>



Comisión Conjunta Sobre

INFORMES ESPECIALES DEL CONTRALOR

de la Asamblea Legislativa del Estado Libre Asociado de Puerto Rico

REQUERIMIENTO DE INFORMACIÓN Y DOCUMENTOS

General Antonio J. Vicéns
Ayudante General
Guardia Nacional de Puerto Rico
San Juan, Puerto Rico

CCSIEC-RID-09-343

La Comisión Conjunta sobre Informes Especiales del Contralor (CCSIEC), creada en virtud de la Ley Núm. 83 del 23 de junio de 1954, tiene como tarea medular efectuar un examen detenido de los Informes del Contralor e investigar cualquier asunto relacionado. Entre otras facultades, la ley antes citada expresamente autoriza a la CCSIEC, so pena de desacato, a citar testigos y solicitar la presentación de documentos y otra evidencia necesaria para realizar sus investigaciones.

La CCSIEC lleva a cabo la Investigación Especial DA-09-03.

En el descargo de nuestras funciones asignadas en la Ley Núm. 83, *supra*, los poderes establecidos en el Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico, así como en las otras disposiciones que rigen nuestro ordenamiento jurídico, **solicitamos copia de los siguientes documentos:**

1. Informe Complementario al PAC (ICP-1).
2. Informe Complementario al PAC (ICP-2).

Se le conceden **diez (10) días**, a partir del recibo de esta notificación, para hacer entrega de los documentos aquí solicitados. Todo documento que pueda considerarse como confidencial, debe estar debidamente identificado como tal para que la CCSIEC garantice y proteja dicha confidencialidad y los derechos procedentes.

La Ley Núm. 83, *supra*, establece que cualquier persona que se niegue a cumplir o deje de cumplir, o impida el cumplimiento de una orden de la Comisión bajo las disposiciones de ésta, incurrirá en desacato y será procesada y castigada en la forma que determine la Ley.

Por la autoridad que le confiere la Ley Núm. 83, *supra*, al Presidente de la Comisión Conjunta sobre Informes Especiales del Contralor, firmo el presente documento hoy, 15 de septiembre de 2009 en San Juan, Puerto Rico.

Carlos J. Torres Torres
Presidente

2009 SEP 24 AM 11:14

DIVISION DE SERVICIOS
ADMINISTRATIVOS
RECIBIDO

¡ATENCIÓN!

SI POR ALGUNA RAZÓN, IMPEDIMENTO O CONDICIÓN FÍSICA, USTED NECESITA TRATO O ASISTENCIA ESPECIAL, FAVOR DE LLAMAR A LOS SIGUIENTES NÚMEROS TELEFÓNICOS: (787) 724-3010 / (787) 977-7785

NUESTRO PERSONAL LE ATENDERÁ Y ASISTIRÁ PARA QUE PUEDA CUMPLIR CON LO SOLICITADO EN ESTE REQUERIMIENTO DE INFORMACIÓN Y DOCUMENTOS.

LA SEDE DE NUESTRAS OFICINAS ESTÁ UBICADA EN EL EDIFICIO 150 DE LA AVENIDA CONSTITUCIÓN,
PASEO COVADONGA, SAN JUAN, PUERTO RICO.



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTELES GENERALES DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



Hon. Luis G. Fortuño Bursat
Gobernador

(787) 289-1400

29 de octubre de 2009

Sr. Manuel Díaz Saldaña
Contralor de Puerto Rico
Oficina del Contralor

Estimado señor Díaz Saldaña:

Le incluyo el Informe Complementario al Plan de Acción Correctiva (ICP-2) correspondiente al Informe de Auditoría DA-09-03, de la Guardia Nacional de Puerto Rico.

Con la implementación del Plan de Acción Correctiva tomaremos las medidas necesarias para corregir las deficiencias señaladas.

Cualquier Información adicional, puede solicitarla al Sr. Víctor M. Ortiz, Oficial Ejecutivo para Asuntos Estatales al (787) 721-3131, extensión 7001.

Cordialmente,

Antonio J. Vicens
General de División (PR), GNPR
Ayudante General

Anejos



INFORME COMPLEMENTARIO AL PLAN DE ACCIÓN CORRECTIVA

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

Entidad Núm: 1422 Informe de Auditoría Núm: DA-09-03 Fecha: 11 de agosto de 2008

Funcionario principal: Antonio J. Vicens Periodo auditado: 1 de julio de 1999 al 30 de junio de 2006

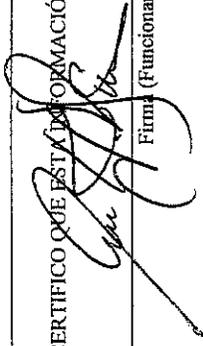
Funcionario designado: Victor M. Ortiz Puesto: Oficial Ejecutivo para Asuntos Estatales Teléfono: (787) 721-3131 Ext. 7001

Indique: PAC ICP Fecha de vencimiento: 1 de noviembre de 2009

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>1. Promulgar procedimientos escritos para regular los procesos relacionados con el control de los activos fijos, el nombramiento del Encargado de la Propiedad y las funciones de éste, la toma de inventarios físicos periódicos y la disposición de la propiedad, entre otros asuntos. [Hallazgo 2-a.1)]</p> <p>3.a.2) El Encargado de la Propiedad:</p> <p>a) Notifique a la Oficina del Contralor y al Departamento de Hacienda, dentro del término establecido, cualquier irregularidad relacionada con la propiedad y los fondos públicos. [Hallazgo 1-a.1) y 2)]</p>	<p>Se redactaron los procedimientos internos de la Sección de Servicios Generales en los cuales se regula el control de los activos fijos, la toma de inventarios físicos anuales y la disposición de la propiedad excedente. El mismo fue firmado por el Ayudante General con vigencia del 27 de octubre de 2009.</p> <p>Se le impartieron instrucciones por escrito al Encargado de la Propiedad para que se asegure de notificar a la Oficina del Contralor y al Departamento de Hacienda cualquier irregularidad relacionada con la propiedad y los fondos públicos según establecido en la reglamentación vigente. Además se promulgó un procedimiento interno que asegura la realización de la investigación y la notificación de la irregularidad a las agencias pertinentes durante el periodo establecido por la reglamentación. El Oficial Ejecutivo para Asuntos Estatales velará por el fiel cumplimiento con la Reglamentación vigente.</p>	<p>Cumplimentado</p> <p>Cumplimentado</p>

(Véase instrucciones al dorso)

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA



Firma (Funcionario Principal)

Fecha

INFORME COMPLEMENTARIO AL PLAN DE ACCIÓN CORRECTIVA (Continuación)

Entidad Auditada:

GUARDIA NACIONAL DE PUERTO RICO

RECOMENDACION	ACCION CORRECTIVA	RESULTADO
<p>d) Concilie los inventarios físicos contra los registros internos de propiedad, y en casos de diferencias, se tomen las medidas que correspondan. [Hallazgo 2-a.5)]</p> <p>e) Exprima los recibos por propiedad en uso (Modelo SC-1211) a todos los funcionarios y empleados de la entidad que tengan unidades de propiedad asignadas, y los mantenga al día. [Hallazgo del 2-a.6(a) al c)]</p>	<p>Se promulgó un procedimiento interno que incluye las normas de control interno y la contabilidad del activo fijo, la toma de inventario anual y la conciliación de este con el Registro de la Propiedad.</p> <p>Se redactó un procedimiento interno que incluye las normas de control interno y la contabilidad del activo fijo, la toma de inventario anual y la conciliación de este con el Registro de la Propiedad. De igual manera establece los procedimientos para la expedición de los recibos de propiedad en uso (Modelo SC-1211) y el proceso para notificar el movimiento y transferencia de equipos entre unidades y empleados de la agencia para mantener al día los registros. Dicho procedimientos entró en vigor el 27 de octubre de 2009.</p>	<p>Cumplimentado</p> <p>Cumplimentado</p>
<p>4. Tomar las medidas necesarias para que se designe un empleado para ejercer las funciones de Administrador de Documentos, en ausencia del Administrador en propiedad. [Hallazgo 5-a.]</p>	<p>El 14 de agosto de 2008 el Oficial Ejecutivo para Asuntos Estatales solicitó a la Oficina de Gerencia y Presupuesto la autorización para el nombramiento de un Administrador de Documentos, sin embargo, dicha solicitud fue denegada. La agencia no cuenta con el personal suficiente para reasignar estas funciones. La ley 7 de 9 de marzo de 2009 inhabilita a la agencia de hacer nombramientos por los próximos 2 años. No obstante, se dará seguimiento para realizar el nombramiento a la mayor brevedad.</p>	<p>Parcialmente Cumplimentado</p>

[Handwritten Signature]
 Iniciales



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTELES GENERALES DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



Hon. Luis G. Fortuño Bursset
Gobernador

(787) 289-1400

12 de enero de 2010

Sr. Manuel Díaz Saldaña

Contralor de Puerto Rico

Oficina del Contralor

P. O. Box 366069

San Juan, Puerto Rico 00936

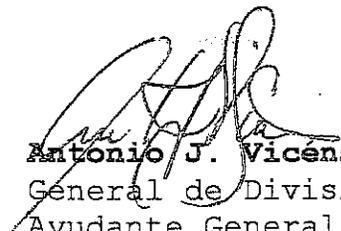
Estimado señor Díaz:

Le incluyo el Plan de Acción Correctiva (OC-DA-10-08), correspondiente al Informe de Auditoría DA-09-03, de la Guardia Nacional de Puerto Rico.

Con la implementación del Plan de Acción Correctiva tomaremos las medidas necesarias para corregir las deficiencias señaladas. Le daremos el seguimiento planificado de acuerdo a las normas y los Reglamentos aplicables.

Cualquier información adicional, puede solicitarla al Sr. Víctor M. Ortiz, Oficial Ejecutivo para Asuntos Estatales al (787) 721-3131, extensión 7001.

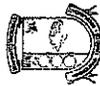
Cordialmente,



Antonio J. Vicéns

General de División, GNPR
Ayudante General

Anejos



PLAN DE ACCIÓN CORRECTIVA

Entidad Auditada: GUARDIA NACIONAL DE PUERTO RICO

Entidad Núm: _____

1422

Informe de Auditoría Núm: DA-10-08

Fecha: 7 de enero de 2010

Funcionario principal: GEN. ANTONIO J. VICENS

Período auditado: 1 de julio

de 1999 al 30 de junio de 2006

Funcionario designado: VICTOR M. ORTIZ

Puesto: ASUNTOS ESTATALES

Teléfono: (787) 721-3131 Ext. 7000

Indique: PAC ICP-1

Fecha de vencimiento: 1 de enero de 2010

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>I. Hallazgo 1 y 2 Pagos Indebidos</p> <p>Tomar las medidas que correspondan y determinar si procede reclamar a los funcionarios responsables de los pagos indebidos por \$175,308.00.</p>	<p>Se le solicitó al Secretario de Justicia que determine si procede reclamar a los funcionarios Responsables de los pagos indebidos por \$175,308.00. (Ver comunicación al Licenciado Antonio M. Sagardía, del 15 de octubre de 2009)</p>	<p>Parcialmente Cumplimentado. Estamos en espera de la determinación del Secretario de Justicia sobre el status de la evaluación y si procede o no el recobro de los pagos indebidos. El Oficial Ejecutivo para Asuntos Estatales tomo las medidas para ejercer la fiscalización eficaz y adecuada al personal bajo su supervisión. Se tomaran las medidas necesarias para que no se repitan situaciones de pagos indebidos.</p>

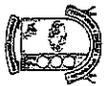
(Véase instrucciones al dorso)

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA

ANTONIO J. VICENS
General de División, GNPR, Ayudante General
Firma (Funcionario Principal)

7 de enero de 2010

Fecha



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

2) La Oficial de Licencia y Asistencia:

a) Hallazgo 2-1. Verifique que el Record de Asistencia Semanal (Modelo SC-1078) esté firmado por el Director de Recursos Humanos o su representante autorizado como constancia de que verificó que el mismo está correcto.

En la actualidad, el Director de Recursos Humanos firma el Modelo SC-1078, Hoja de Asistencia Semanal como constancia de que verificó que el mismo está correcto. Se preparará el Manual de Procedimientos para regir las actividades relacionadas a la Hoja de Asistencia Semanal de los empleados irregulares. Se ofrecerá adiestramiento al Oficial de Licencia y Asistencia para que adquiera los conocimientos necesarios para la elaboración del Manual de Procedimientos para regir las operaciones del personal irregular.

No obstante, con el objetivo de agilizar los procesos de asistencia y licencias, se ha implementado un sistema electrónico para el registro y manejo de la asistencia y licencias de todos los empleados.

b) Hallazgo 2b. Considere para el cómputo de las horas trabajadas por el personal irregular, los días en que éstos estuvieron en licencias por vacaciones y por enfermedad.

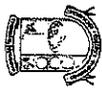
Actualmente la Agencia no tiene personal irregular, no obstante, se instruyó a la Oficial de Licencia y Asistencia que, de surgir nombramientos irregulares debe tomarse en consideración el periodo en que el personal irregular esté en disfrute de alguna licencia concedida. Además, se instruyó a la Oficial de Licencia y Asistencia a establecer los procedimientos y normas de trabajo para regir las operaciones relacionadas con el personal irregular.

Parcialmente Cumplimentada. Se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado el adiestramiento para la Oficial de Licencia y Asistencia de "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios para la elaboración del mismo. Estos adiestramientos se ofrecerán en el próximo Calendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010.

Estamos en el proceso de la redacción del Reglamento del Sistema Biométrico para establecer las Normas y Procedimientos a seguir en la Administración de los Procesos de Asistencia y Licencias.

Parcialmente Cumplimentada. Se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado el adiestramiento para la Oficial de Licencia y Asistencia de "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios para la elaboración de procedimientos escritos para regir las operaciones relacionadas con el personal irregular. Estos adiestramientos se ofrecerán en el próximo Calendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010. Se está en proceso de la redacción del Reglamento del Sistema Biométrico para establecer las Normas y Procedimientos a seguir en la Administración de los Procesos de Asistencia y Licencias.

ASL
Iniciales



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

<p>c) Hallazgo 5-a.1 Requiera a los Supervisores de las distintas armerías que entregan cheques de sueldo a empleados irregulares, la devolución del documento interno <i>Entrega de Cheques</i> como evidencia de que entregaron los mismos. Además, vea que dicho documento esté firmado por los empleados.</p>	<p>En la actualidad la Agencia no tiene personal irregular, no obstante de surgir nombramientos irregulares, los cheques serán entregados por la Sección de Finanzas y Presupuestos a quienes se les delegó la entrega de cheques.</p>	<p>Cumplimentada. Todos los cheques serán entregados por la Sección de Finanzas y Presupuesto y están custodiados bajo llave en una caja fuerte.</p>
<p>c) Hallazgo 5-a.2 Mantenga en un lugar seguro bajo llave o caja fuerte los cheques de nómina que se reciben.</p>	<p>Actualmente los cheques de nómina están bajo la custodia de la Sección de Finanzas y Presupuesto en una caja fuerte bajo llave y no tenemos empleados irregulares.</p>	<p>Cumplimentada. Todos los cheques son entregados por la Sección de Finanzas y Presupuesto.</p>
<p>3) Hallazgo 3 -- El empleado a cargo del proceso de liquidación de licencias de personal irregular cumpla con lo establecido en la Ley y reglamentación, de manera que se retenga al empleado el importe de las deudas que éste tenga con el Gobierno y lo remese al Secretario de Hacienda.</p> <p>4) Al personal a cargo de la administración del personal irregular:</p> <p>a) Hallazgo 4-a. Mantenga expedientes completos y organizados de los documentos relacionados con éstos, de manera que se corrijan y no se repitan las situaciones comentadas en el Hallazgo 4-a.</p>	<p>Se instruyó al Oficial de Nóminas a cumplir con lo establecido en la Ley Núm. 230 y a las Cartas Circulares del Departamento de Hacienda con relación al pago global de licencias acumuladas y para liquidar deudas contributivas mediante descuento en el referido pago.</p>	<p>Cumplimentada. Actualmente la Agencia no tiene personal irregular nombrado. No obstante, se instruyó a con la Oficina de Recursos Humanos que debe cumplir con la reglamentación para la liquidación de las deudas en todos los pagos globales. La Oficial de Nóminas participó de los adiestramientos ofrecidos por el Departamento de Hacienda.</p>
<p>a) Hallazgo 4-a. Mantenga expedientes completos y organizados de los documentos relacionados con éstos, de manera que se corrijan y no se repitan las situaciones comentadas en el Hallazgo 4-a.</p>	<p>Se instruyó a la empleada a cargo de los Expedientes de Personal Irregular a la revisión de los mismos de manera tal que estén completos y organizados. Además, a establecer los procedimientos y normas de trabajo para regir las operaciones relacionadas con documentos necesarios para efectuar nombramientos de personal irregular.</p>	<p>Parcialmente Cumplimentada. Actualmente la Agencia no tiene personal irregular nombrado. No obstante, se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado el adiestramiento para el (la) empleado (a) a cargo de la administración del personal irregular de: "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios</p>



<p>b) Obtenga las Autorizaciones Fiscales previo a los nombramientos de éstos (Hallazgo 4-b.1) e incluyan en los expedientes de personal dichas autorizaciones como evidencia de la disponibilidad de fondos para el pago de las nóminas (Hallazgo 4-b.2)</p>	<p>Actualmente la Agencia no tiene personal irregular. Se instruyó a la empleada a cargo de Nombramientos y Cambios a establecer los procedimientos y normas de trabajo para regir las operaciones relacionadas con el personal irregular donde incluya evidencia de que la Agencia cuenta con los Fondos necesarios para efectuar el nombramiento.</p>	<p>para la elaboración de procedimientos escritos para regir las operaciones relacionadas con el personal irregular. Estos adiestramientos se ofrecerán en el próximo Calendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010.</p> <p>Parcialmente Cumplimentada. Se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado para el (la) empleado (a) a cargo de la administración del personal irregular el adiestramiento de: "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios para la elaboración de procedimientos escritos para regir las operaciones relacionadas con el personal irregular. Estos adiestramientos se ofrecerán en el próximo Calendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010.</p>
<p>c) Requiera a los empleados que cesan en el servicio que sometan las certificaciones de deuda por propiedad inmueble o mueble, de pensión alimentaria y de deuda por contribuciones sobre ingresos antes de procesar el pago global de las licencias acumuladas. Además, vea que se les retenga cualquier cantidad adeudada y que se haga la remesa a las agencias correspondientes. (Hallazgo del 4-c.1 al 3)</p>	<p>Se instruyó a la empleada a cargo de Nombramientos y Cambios y al Oficial de Nóminas a establecer los procedimientos y normas de trabajo para regir las operaciones relacionadas con el personal irregular donde incluya hoja de control relacionada a los documentos necesarios para procesar el pago global de las licencias acumuladas.</p>	<p>Parcialmente Cumplimentada. Se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado para el (la) empleado (a) a cargo de la administración del personal irregular el adiestramiento de: "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios para la elaboración de procedimientos escritos para regir las operaciones relacionadas con el personal irregular. Estos adiestramientos se ofrecerán en el próximo Calendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010.</p>

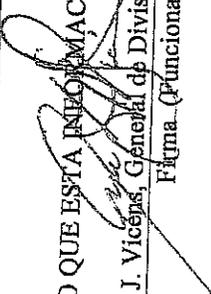
[Handwritten Signature]
Iniciales



<p>d) Tome las medidas necesarias para que el Record de Licencia - Personal Irregular (Modelo SC-1090) y el Modelo SC-1078 se archiven en forma segura y ordenada para que puedan ser localizados sin dificultad (Hallazgo 4-d)</p>	<p>Se preparará el Manual de Procedimientos para registrar las actividades relacionadas a la Hoja de Asistencia Semanal (Modelo SC-1078) y Modelo SC-1090 de los empleados irregulares. Se ofrecerá adiestramiento al Oficial de Licencia y Asistencia para que adquiera los conocimientos necesarios para la elaboración del Manual de Procedimientos para registrar las operaciones del personal irregular. Actualmente no tenemos personal irregular.</p>	<p>Parcialmente Cumplimentada. Se coordinará con la Oficina de Recursos Humanos del Estado Libre Asociado el adiestramiento para la Oficial de Licencia y Asistencia de "La Organización y Redacción de Procedimientos" y "Preparación de Manual de Procedimientos" a los fines de que adquiera los conocimientos necesarios para la elaboración del mismo. Estos adiestramientos se ofrecerán en el próximo Catendario de Adiestramiento que cubre el periodo del 1 de enero al 30 de junio de 2010.</p>
---	--	---

(Véase instrucciones al dorso)

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA

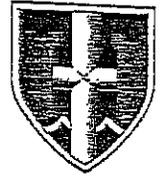

Antonio J. Vicéns, General de División, GNPR, Ayudante General
Firma (Funcionario Principal)

7 de enero de 2010
Fecha

Iniciales



ESTADO LIBRE ASOCIADO DE PUERTO RICO
GUARDIA NACIONAL DE PUERTO RICO
CUARTELES GENERALES DE FUERZA CONJUNTA
OFICINA DEL AYUDANTE GENERAL
P.O. BOX 9023786, SAN JUAN, PUERTO RICO 00902-3786



Hon. Luis G. Fortuño Bursat
Gobernador

(787) 289-1400

15 de octubre de 2009

Hon. Antonio M. Sagardía De Jesús
Secretario de Justicia
Departamento de Justicia
P.O. Box 9020192
San Juan, PR 00902-0192

Estimado señor Secretario:

El 28 de septiembre recibimos el Informe de Auditoría DA 10-08 de la Oficina del Contralor del 25 de septiembre de 2009.

En el mismo se recomendó que el Departamento de Justicia considere los hechos que se comentan en el hallazgo 1 del informe y determine si procede reclamar a los funcionarios responsables los pagos indebidos por \$175,308.00 mencionados en dicho hallazgo.

Sobre este particular, nos interesa conocer cuál es el estatus de dicha evaluación y si procede o no el recobro de esos dineros.

Cualquier comunicación sobre este particular, puede referirla al coronel retirado Víctor M. Ortiz, Oficial Ejecutivo para Asuntos Estatales al (787) 289-1400 ext. 7000.

Cordialmente,

Antonio J. Vicéns
General de División (PR), GNPR
Ayudante General

comentarios se consideran al revisar el borrador del informe y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN LA GUARDIA NACIONAL DE PUERTO RICO de forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, éste prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

HALLAZGOS EN LA GUARDIA NACIONAL DE PUERTO RICO

Los hallazgos 1 y 2 se clasifican como principales y los enumerados del 3 al 5, como secundarios.

Rec Humanos
Hallazgo 1 - Nombramientos de empleados en puestos irregulares que pasaron a ocupar puestos en el servicio de carrera sin cumplir con el tiempo requerido por ley y otras deficiencias relacionadas

a. Los asuntos relacionados con el personal irregular son administrados por la Oficina de Recursos Humanos³. Además, ésta tenía la responsabilidad de mantener los documentos y la información relacionados con los nombramientos de los empleados irregulares que pasaban a ocupar puestos en el servicio de carrera. La Directora de Recursos Humanos supervisaba dichas operaciones y le respondía al Oficial Ejecutivo para Asuntos Estatales.

Del 1 de julio de 2000 al 30 de junio de 2004, según información provista por la Directora de Recursos Humanos, la Guardia Nacional realizó 37 nombramientos de personal irregular. En los años fiscales del 2000-01 al 2003-04 la Guardia Nacional efectuó desembolsos por nóminas y costos relacionados con el personal irregular por \$218,489⁴, según información provista por el Director de Finanzas y Presupuesto.

³ Los controles administrativos relacionados con las operaciones de recursos humanos se comentan en el Informe de Auditoría DA-09-25.

⁴ El pago de nómina provenía de aportaciones federales (*Cooperative Funding Agreement*) o de un pareo de fondos (75 por ciento del Fondo Federal y el otro 25 por ciento del Fondo General) asignados al Gobierno mediante resoluciones conjuntas estatales para el Programa de Seguridad y Conservación de Facilidades Militares.



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: DA-09-03 Número de unidad: 1422 Entidad auditada: Guardia Nacional de Puerto Rico

Fecha del Informe: 11 de agosto de 2008 Período auditado: 1 de julio de 1999 al 30 de junio de 2006

Indique: PAC ICP - 3

Funcionario enlace: Gen. Antonio J. Vicéns Puesto: General de División, GNPR, Ayudante General Teléfono: 289-1631

Funcionario principal o su representante autorizado: Victor M. Ortiz Puesto: Oficial Ejecutivo para Asuntos Especiales Teléfono: (787) 721-3131 Ext. 7000

Fecha: 1 de marzo de 2010

[Signature]
 Antonio J. Vicéns
 Firma del funcionario principal o su representante autorizado

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>Promulgar normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional (Hallazgo 1-a.1).</p> <p>Para la administración, la seguridad y el uso de los sistemas computerizados (Hallazgo 5-a.1)</p>	<p>Con el propósito de establecer procedimientos por escrito para regir la contabilidad de la Guardia Nacional se estableció el Programa MIP Fund Accounting y se creó un Manual de Procedimientos de Contabilidad y se Implantó un Sistema de Requisiciones Electrónicas y Ordenes de compras Microix.</p> <p>Para la administración, la seguridad y el uso de los sistemas computerizados se estableció por escrito las normas y procedimientos y esta en evaluación por la División Legal.</p>	<p>Cumplimentado se estableció un nuevo Sistema de Contabilidad (Programa MIP Fund Accounting) y se creó un Manual de Procedimientos de Contabilidad. Además, se implantó un sistema electrónico para las requisiciones y las ordenes de compra. (Véase Anejo I)</p> <p>Parcialmente Cumplimentado el Reglamento del Uso y Manejos de los Recursos de Informática esta en revisión y próximamente será sometido para la revisión y aprobación del Ayudante General. (Véase Anejo II)</p>



PLAN DE ACCIÓN CORRECTIVA (Continuación)

Entidad Auditada: Guardia Nacional de Puerto Rico

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>2. Tomar las medidas necesarias para que se cumplan con las disposiciones de las Leyes Aplicables a los single audits y que no se repitan las situaciones comentadas.</p>	<p>Se estableció un Contrato de Servicios Profesionales con el CPA López Vega para realizar una evaluación de riesgos y de procesos. Además, se Ocupo el puesto de Auditor Interno.</p>	<p>Cumplimentada Se estableció un Manual sobre riesgos y procesos, se tomaran las medidas correctivas de una forma eficiente y rápida. Con este sistema se corregirán los diferentes hallazgos.</p>
<p>3. Ver que se atiendan las recomendaciones de los informes de los single audits de los años fiscales 1999-00 al 2002-03, y anos siguientes. (Hallazgos 3-a.1)</p>	<p>Con la implantación de las recomendaciones de las diferentes áreas Finanzas, Recursos Humanos y Servicios Generales. Con este sistema se corregirán los hallazgos y evitaremos que se repitan.</p>	<p>Cumplimentado se estableció el Manual de Contabilidad. Además, del Manual de riegos y Procesos.</p>
<p>4. Ver que el Comité de Ética de la Guardia Nacional y el Oficial Ejecutivo para Asuntos Estatales cumplan con sus responsabilidades de velar porque se atiendan las recomendaciones de los informes de los single audits.</p>	<p>Se creo un nuevo Comité de Ética en la Agencia. También, se le entregó copia de los resultados de las auditorias para que se cumpla con las recomendaciones de los Hallazgos. El Oficial Ejecutivo para Asuntos Estatales velará por que se cumpla con las recomendaciones de los informes de single audits. Además, vigilará que se cumpla con toda la reglamentación vigente en todas las áreas.</p>	<p>Cumplimentado. Se constituyó un nuevo Comité de Ética. Se establecieron los Manuales de Contabilidad y de Riegos y Procesos. Con la implantación y supervisión eficaz del personal velará que se cumpla con la Ley, los reglamentos y las normas de una sana administración</p>

[Handwritten Signature]

Oficiales



PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>5. Ver que el Oficial Ejecutivo para Asuntos Estatales cumpla con su responsabilidad y ejerza una supervisión eficaz del personal, y se asegure de que:</p> <ul style="list-style-type: none"> a) El Director de Finanzas y Presupuesto cumpla con las disposiciones de ley y los reglamentos, las normas de sana administración, el control interno y se asegure de que: <ol style="list-style-type: none"> 1. Los contadores: <ul style="list-style-type: none"> a) Consoliden todos los datos financieros en el sistema <i>Micro Information Product (MIP)</i>, de manera que se pueda ofrecer información financiera confiable. b) Mantengan un registro de las cuentas por cobrar en el Módulo del Mayor General del Sistema MIP que incluya, entre otras cosas, el número de objeto, nombre del proveedor, fecha de la factura al cobro emitida, y que realicen análisis de dichas cuentas de acuerdo con la fecha de vencimiento. (Hallazgo 1-a.4) 	<p>Efectivo el 26 de enero de 2009, se autorizó a cubrir el puesto de Oficial Ejecutivo para Asuntos Estatales. Dicho funcionario ha realizado una supervisión efectiva, para corregir las diferentes deficiencias en el Área de Finanzas y Presupuestos. Estas incluyen utilizar el Sistema de Contabilidad MIP en su mayor capacidad.</p> <p>Para lograrlo se estableció n nuevo Sistema de Contabilidad. Se oriento y adiestro a los Contadores de la Oficina de Finanzas, para que utilicen el Sistema MIP uniformemente y que se corrija la información financiera suministrada.</p> <p>Además, se están realizando las entradas al Sistema MIP de las Facturas al Cobro y se harán las gestiones de cobro de manera efectiva, según el Reglamento Num. 44 "Deudas no Contributivas Existentes a Favor del Gobierno de Puerto Rico".</p>	<p>Cumplimentado. Se estableció el Manual del Sistema de Contabilidad y el Manual de Riesgos, de esta forma estableceremos una contabilidad confiable.</p> <p>Cumplimentado se implantó un Manual de Procedimientos de Contabilidad el cual servirá de guía en la operación del Sistema de Contabilidad en la Agencia. Se implantó el Manual de Procedimientos para los diferentes procesos y riesgos en todas las áreas.</p> <p>Cumplimentado las Facturas al Cobro se están registrando en el Sistema de MIP y se realizan las gestiones de cobro, según lo establece el Reglamento 44, para esos fines.</p>

ADJ.
Iniciales



PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>c) Realicen gestiones de cobro efectivas, dentro del término requerido para ello, y se utilice el formulario correspondiente (Hallazgo 4-a.1)</p> <p>d) Realicen análisis de las facturas al cobro cuyas gestiones de cobro resulten infructuosas y se refieran al Departamento de Hacienda o al Secretario de Justicia, según corresponda. (Hallazgo 4-a.2)</p>	<p>Cuando el Contador reciba las Facturas al Cobro se entraran al Sistema MIP, y se realizarán las gestiones de cobro dentro del termino requerido de acuerdo a la Reglamentación Núm. 44.</p> <p>El Contador I, a cargo de entrar las facturas al cobro al Sistema MIP, emitirá un informe detallado, para evaluar si las mismas se referirán al Departamento de Justicia o al Departamento de Hacienda, según sea el caso.</p>	<p>Cumplimentado estamos realizando las entradas al Sistema MIP de las Facturas al Cobro y se harán las gestiones de cobro de manera efectiva, según el Reglamento Núm. 44.</p>
<p>2. La Directora Auxiliar de Finanzas y Presupuesto registre con prontitud los comprobantes de pago correspondientes a los fondos de Mejoras Permanentes en e Sistema de Contabilidad mecanizado MIP y que no se repitan situaciones como la comentada en el Hallazgo 1-a.3.</p>	<p>Actualmente la Directora Auxiliar de Finanzas y Presupuesto mantiene sus registros y las conciliaciones de las Mejoras Permanentes debidamente actualizado.</p>	<p>Cumplimentado se evaluaran todas las Facturas al Cobro y cuando las gestiones de cobro sean infructuosas se referirán al Departamento de Justicia o al Departamento de Hacienda, según sea el caso.</p> <p>Cumplimentado. Su oficina le dará seguimiento a los registros y conciliaciones de las mejoras Permanentes, no obstante, la Directora Auxiliar de Finanzas y Presupuesto fue instruida a que mantenga los registros de contabilidad de las mismas debidamente actualizada.</p>

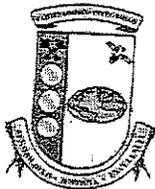
[Handwritten Signature]
Jefes
Jefes



PLAN DE ACCIÓN CORRECTIVA (Continuación)

RECOMENDACION	ACCION CORRECTIVA	RESULTADO
<p>a. El Oficial Principal de Informática:</p> <p>1) Mantenga los respaldos de la información almacenada en los medios electrónicos en un lugar seguro fuera de los predios de la Agencia. (Hallazgo 5-a.2)</p> <p>2) Prepare, para la aprobación del Ayudante General, un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. (Hallazgo 5-a.3).</p>	<p>Referente a la información almacenada en medios electrónicos, le informó que según certificación emitida por el Coronel Retirado Ramón L. Díaz Santiago, Oficial Administrativo del Comando, de la Guardia Nacional los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto Rico se mantienen almacenados bajo llave en la Oficina de la Guardia Estatal, esta oficina quedan ubicada en la Base de Isla Grande, fuera de los predios de nuestra Agencia. Por tal razón, damos por corregido dicho hallazgo.</p> <p>Con relación a la implementación del Plan de Contingencia, se encuentra el evaluación del Asesor Legal para finalmente pasar para la aprobación del Ayudante General.</p>	<p>Cumplimentado con relación a el hallazgos de los <i>Back up</i> de la Oficina de Informática, este fue corregido, según comunicación recibida de sus oficinas el 26 de noviembre de 2008.</p> <p>Parcialmente cumplimentado el desarrollo de un Plan de Contingencia aún se encuentra en evaluación del Asesor Legal y para la aprobación del Ayudante General. Además, de la creación del Manual de Procedimientos Internos de esa Oficina.</p>

[Signature]
Iniciales



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

14 de mayo de 2010

vortiz@gopr.gobierno.pr

Gen. Antonio J. Vicens González
Ayudante General
Guardia Nacional
San Juan, Puerto Rico

Estimado general Vicens González:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-3)* que nos remitió el 18 de marzo sobre el *Informe de Auditoría DA-09-03* de la Guardia Nacional de Puerto Rico (Guardia Nacional). Determinamos que las **recomendaciones 1 y 5.b.2)** se consideran parcialmente cumplimentadas. A la **Recomendación 1**, respecto a las normas y procedimientos escritos para regir la contabilidad de la Guardia Nacional [**Hallazgo 1-a.1)**], no le daremos seguimiento. Las medidas tomadas para cumplimentar esta última se verificarán en la próxima auditoría de dicha unidad.

En el *ICP-4* deberá suministrarlos la siguiente información y documentos:

1. Evidencia de la aprobación del *Reglamento del Uso y Manejo de los Recursos de Informática*. [**Hallazgo 5-a.1)**] [**Recomendación 1)**]
2. Evidencia de la aprobación del Ayudante General de un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. [**Hallazgo 5-a.3)**] [**Recomendación 5.b.2)**]

Agradeceremos que nos remita el *ICP-4* con la información y los documentos solicitados, no más tarde del 1 de septiembre de 2010, mediante el Sistema PAC que está localizado en nuestra página en Internet: <http://www.ocpr.gov.pr>, y según las instrucciones incluidas en la *Carta Circular OC-10-08* del 21 de octubre de 2009. La información incluida en el *ICP-4* estará sujeta a corroboración por esta Oficina.

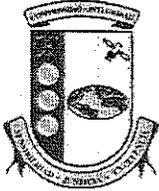
Para información adicional, el funcionario designado por usted puede comunicarse con la Sra. Maria del Carmen Alvarado Pacheco, Analista del Plan de Acción Correctiva, al (787) 294-1991, extensión 550.

PO BOX 366069 SAN JUAN, PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: <http://www.ocpr.gov.pr>



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

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
<p>a. El Oficial Principal de Informática:</p> <p>1) Mantenga los respaldos de la información almacenada en los medios electrónicos en un lugar seguro fuera de los predios de la Agencia. (Hallazgo 5-a.2)</p> <p>2) Prepare, para la aprobación del Ayudante General, un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. (Hallazgo 5-a.3).</p>	<p>Referente a la información almacenada en medios electrónicos, le informo que según certificación emitida por el Coronel Retirado Ramón I. Díaz Santiago, Oficial Administrativo del Comando, de la Guardia Nacional los "Tape Back up" del Área de Informática de Servicios Administrativos de la Guardia Nacional de Puerto Rico se mantienen almacenados bajo llave en la Oficina de la Guardia Estatal, esta oficina quedan ubicada en la Base de Isla Grande, fuera de los predios de nuestra Agencia. Por tal razón, damos por corregido dicho hallazgo.</p> <p>Con relación a la implementación del Plan de Contingencia, se realizaron las coordinaciones pertinentes para establecer el mismo. Actualmente no contamos con el presupuesto para implementarlo. No obstante, estamos realizando las gestiones necesarias de identificar fondos para ese propósito.</p>	<p>Cumplimentado con relación a el hallazgos de los Back up de la Oficina de Informática, este fue corregido, según comunicación recibida de sus oficinas el 26 de noviembre de 2008.</p> <p>Parcialmente cumplimentado el desarrollo de un Plan de Contingencia aún se encuentra en proceso, hasta tanto la Oficina de Gerencia y Presupuesto autorice cubrir la posición de Oficial de Informática, ya que hemos identificado fondos para ese propósito. Además, de la creación del Manual de Procedimientos Internos de esa Oficina.</p>



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

21 de octubre de 2010

vortiz@gnpr.gobierno.pr

Gen. Antonio J. Vicens González
Ayudante General
Guardia Nacional
San Juan, Puerto Rico

Estimado general Vicens González:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-4)* que nos remitió el 15 de octubre de 2010 sobre el *Informe de Auditoría DA-09-03* de la Guardia Nacional de Puerto Rico (Guardia Nacional). Determinamos que las **recomendaciones 1 y 5.b.2)** se consideran parcialmente cumplimentadas.

En el *ICP-5* deberá suministrarnos la siguiente información y documentos:

1. Evidencia de la aprobación del *Reglamento del Uso y Manejo de los Recursos de Informática*. [**Hallazgo 5-a.1)**] [**Recomendación 1**]
2. Evidencia de la aprobación del Ayudante General de un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. [**Hallazgo 5-a.3)**] [**Recomendación 5.b.2)**]

Agradeceremos que nos remita el *ICP-5* con la información y los documentos solicitados, no más tarde del 1 de febrero de 2011, mediante el Sistema PAC que está localizado en nuestra página en Internet: <http://www.ocpr.gov.pr>, y según las instrucciones incluidas en la *Carta Circular OC-10-08* del 21 de octubre de 2009. La información incluida en el *ICP-5* estará sujeta a corroboración por esta Oficina.

Para información adicional, el funcionario designado por usted puede comunicarse con el Sr. Pedro J. Collado León, Analista del Plan de Acción Correctiva, al (787) 294-1991, extensión 518.

Gen. Antonio J. Vicens González

Página 2

21 octubre de 2010

Contamos con su cooperación para mejorar la fiscalización y la administración de la propiedad y de los fondos públicos.

Cordialmente,



Antonio Olmo Vázquez

Director

División "A" de Auditorías
de Departamentos y Agencias

c Hon. Carlos J. Torres Torres
Presidente
Comisión Conjunta sobre
Informes Especiales del Contralor

Sr. Víctor M. Ortiz
Oficial Ejecutivo para Asuntos Estatales
Guardia Nacional de Puerto Rico



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: DA-09-03 Número de unidad: 1422 Entidad auditada: Guardia Nacional de Puerto Rico

Fecha del informe: 11 de agosto de 2008 Periodo auditado: 1 de julio de 1999 al 30 de junio de 2006

Indique: PAC ICP - 4

Funcionario enlace: Víctor M. Ortiz, Coronel (Ret) Puesto: Oficial Ejecutivo para Asuntos Estatales Teléfono: (787) 721-3131 Ext. 7000

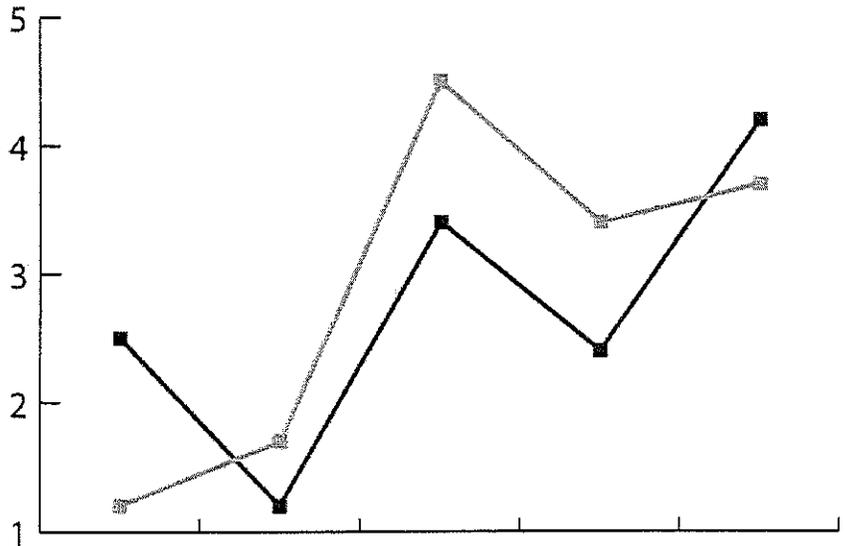
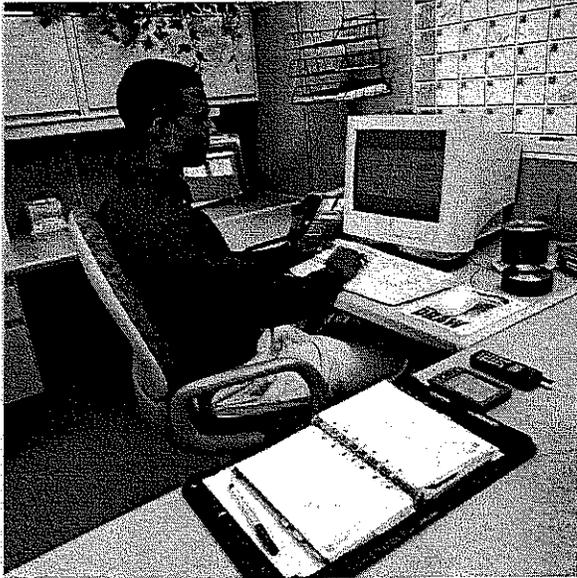
Funcionario principal o su representante autorizado: General Antonio J. Vicéns Puesto: Ayudante General Teléfono: (787) 721-3131 Ext. 1631

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA Antonio J. Vicéns Fecha: 4 de octubre de 2010

Antonio J. Vicéns
 Firma del funcionario principal o su representante autorizado

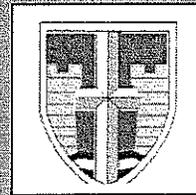
RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
1. Evidencia de la aprobación del Reglamento del Uso y Manejo de los Recursos de Informática. Hallazgo 5-a.1.	Se preparo el Reglamento Sobre el Uso y Manejo de los Sistemas de Información y Tecnología de la Guardia Nacional de Puerto Rico.	Parcialmente Cumplimentado. El Reglamento Sobre el Uso Y Manejo de los Sistemas de Información y Tecnología de la Guardia Nacional de Puerto Rico esta en revisión y evaluación final en la División Legal. (Ver anejo).
2. Evidencia de la aprobación del Ayudante General de un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. Hallazgo 5-a.3	Se preparo el Plan de Continuidad Operacional con las medidas de control a tomarse cumpliendo con las necesidades En casos de emergencia, desastre, fuego o cualquier circunstancia que afecten las operaciones normales en la Agencia.	Parcialmente Cumplimentado. El Plan de Continuidad Operacional esta en los procesos de revisión y evaluación final.

(Véase instrucciones al final del modelo)



*REGLAMENTO SOBRE
EL USO Y MANEJO DE
LOS SISTEMAS DE
INFORMACION Y
TECNOLOGIA DE LA
GUARDIA NACIONAL
DE PUERTO RICO*

BORRADOR EN REVISION
6 DE OCTUBRE DE 2010



ANTONIO J. VICENS
GENERAL DE DIVISION (PR), GNPR
AYUDANTE GENERAL

1 DE NOVIEMBRE DE 2010

I. Introducción

Con el objetivo de agilizar los procesos operacionales, aumentar la eficiencia y efectividad en la prestación de los servicios y viabilizar la interconexión tecnológica entre las agencias, la Guardia Nacional de Puerto Rico ha establecido un Sistema de Información Computadorizado que cuenta con numerosas unidades de equipo, programas, redes de servicios electrónicos internos y acceso al Internet.

La mecanización de los sistemas de información requiere regular el uso apropiado de sus componentes y equipos, e implantar las medidas necesarias para garantizar la confidencialidad de la información.

II. Título

Este documento se conocerá como ***“Reglamento Sobre Uso y Manejo de los Sistemas de Información y Tecnología de la Guardia Nacional de Puerto Rico”***.

III. Base Legal

Este Reglamento se emite conforme a las disposiciones de la Ley número 62 del 23 de junio de 1969, conocida como el Código Militar de Puerto Rico y conforme a La Ley Núm. 151 del 22 de junio de 2004, conocida como “Ley de Gobierno Electrónico” la cual adopta como política pública la incorporación de las tecnologías de información a los procedimientos gubernamentales, a la prestación de servicios, a la difusión de información e implementar las normas y procedimientos que garanticen el uso adecuado, efectivo y seguro de los sistemas de tecnología e información del gobierno de Puerto Rico

IV. Propósito

Este reglamento tiene los siguientes propósitos:

1. Establece las normas y guías a los usuarios de la Agencia a fin de garantizar que el acceso a los sistemas de tecnología, información, Internet y uso de Correo Electrónico sean instrumentos de comunicación relacionados con las funciones de la Agencia.
2. Crea las condiciones necesarias para garantizar que el uso de los sistemas de tecnología e información gubernamental y sus aplicaciones se haga de una forma segura, efectiva y adecuada

BORRADOR

para salvaguardar y proteger la confidencialidad de la información de carácter privilegiado y confidencial que se adquiere, custodia y procesa.

3. Garantizar la exactitud y seguridad en la transferencia de datos a través del sistema de información computadorizado compartido por los organismos gubernamentales.
4. Protege al usuario, la GNPR y al Gobierno de Puerto Rico mediante proscripción de aquella conducta que ponga en riesgo los sistemas y la información que estos contienen.

V. Aplicabilidad

Las normas y prohibiciones establecidas en este Reglamento aplicarán a todos los usuarios del Sistema. Las mismas aplican al manejo de los equipos, componentes y unidades del Sistema, incluyendo computadoras, microcomputadoras, servidores, terminales, redes de comunicación externa e interna, servicios comerciales en línea, archivos computadorizados y medios electrónicos de comunicación que se adopten e incorporen en el futuro. Así mismo, aplica a todos los sistemas, programas (software), piezas y accesorios periferales complementarios, existentes y futuros. Cada usuario es responsable de familiarizarse, conocer y cumplir con las normas aplicables al uso y manejo del Sistema, incluyendo lo relativo a la comunicación electrónica.

VI. Definiciones

1. Acción Disciplinaria - Son las sanciones impuestas por el Ayudante General a un empleado cuando la conducta de un funcionario o empleado no se ajusta a las normas establecidas en las leyes, reglamentos y órdenes administrativas establecidas por la Guardia Nacional.
2. Acuerdo- Entiéndase Acuerdo del Usuario según establecido en este Reglamento.
3. Aplicación – programas o recursos desarrollados para llevar a cabo funciones o usos específicos o para dar apoyo a los procesos organizacionales.
4. Archivos Electrónicos – información almacenada electromagnéticamente en las computadoras y servidores.
5. Agencia- Guardia Nacional de Puerto Rico y sus programas adscritos.

BORRADOR

6. Antivirus- Programa que protege los sistemas de información de los ataques de virus conocidos.
7. Autoridad Nominadora – Ayudante General
8. Cifrar (Encrypt)- Proceso en el cual los datos se convierten a un formato que no puede descifrarse fácilmente por personas no autorizadas a acceder los mismos.
9. Computadora personal – computadora d escritorio o portátil adquirida por la GNPR y asignada a un empleado o empleada con el propósito de mejorar su ambiente de trabajo y mecanizar sus funciones.
10. Contraseña (Password)- Secuencia de caracteres que se utiliza para comprobar que el usuario que ésta requiriendo acceso a un sistema es realmente ese usuario.
11. Correo Electrónico – servicio de envío de mensajes o correspondencia mediante transferencia electrónica a través de una red.
12. Equipos – componentes del sistema, tales como computadoras personales, impresoras, servidores, fotocopiadoras, unidades periferales, tales como monitores, cables, discos.
13. “Firewall” – filtro que controla las comunicaciones que pasan de una red a la otra y permite o deniega las transmisiones para evitar que intrusos puedan acceder información confidencial.
14. Internet – red construida por la interconexión de servidores a nivel mundial que permite a millones de usuarios cruzar fronteras étnicas, idiomáticas y otras, a fin de intercambiar y compartir información mediante diversos servicios disponibles.
15. GNPR – Guardia Nacional de Puerto Rico
16. Oficial Principal- Oficial Principal de Informática de la Guardia Nacional de Puerto Rico.
17. OTI- Oficina de Tecnología e Información de la Guardia Nacional de Puerto Rico.
18. Usuario – Todo funcionario (a), empleado (a), contratista independiente, personal militar y persona debidamente autorizada por el Ayudante General o su representante autorizado o persona

BORRADOR

a quien éste delegue, a tener acceso y utilizar los recursos y servicios del Sistema de Información de la Guardia Nacional de Puerto Rico.

19. Servicio - ellos servicios de Sistemas de Información tales como:
 - A. La utilización de programas de oficina
 - B. Correo Electrónico
 - C. Uso de Impresoras
 - D. Computadoras y sus periferales
 - E. Otros dispositivos conectados a la red de computadoras de la Agencia, el Internet y aquellos otros que resulten en una red de computadoras y datos donde existen dichos servicios de información que estarán disponibles a aquellos usuarios debidamente autorizados.
20. Servidor - computadora en donde se almacenan y se instalan programas y documentos que utilizarán otras computadoras.
21. Sistemas de Información – Sistema de Información Computadorizado, los datos e información almacenados en el mismo, y los servicios de comunicación electrónica y de acceso al Internet implantados en la Guardia Nacional de Puerto Rico y sus programas adscrito.

VII. Responsabilidades

A. Oficina de Tecnología e Información (OTI):

1. Proveer a los usuarios autorizados el acceso apropiado y la configuración de seguridad luego que cada usuario haya firmado el acuerdo que se encuentra anejado en el presente Reglamento.
2. Configuraré el control de acceso, la seguridad, corta fuegos "Firewall" y todas las aplicaciones de Internet.
3. De detectar que la información enviada o recibida por algún usuario cause o tenga la capacidad de causar daño al Estado Libre Asociado de Puerto Rico o a la Agencia, o esté prohibida por ley o reglamento, OTI esta facultado para alterar, remover o grabar dicha información. Una vez ocurra esto, OTI recopilará toda la evidencia disponible y la referirá al supervisor de dicho usuario para su evaluación. De determinarse que existe una infracción a este Reglamento el supervisor enviara este asunto

BORRADOR

a la Oficina de Recursos Humanos para el inicio de la acción disciplinaria correspondiente.

B. Supervisores:

1. Seleccionarán los usuarios y determinarán los accesos apropiados y la seguridad requerida por ellos.
2. Supervisará el uso correcto de los sistemas de tecnología e información de sus empleados.
3. Referirá a la Oficina de Recursos Humanos para el inicio de la acción administrativa correspondiente en aquellos casos en donde se haya cometido una infracción a este reglamento.

C. Usuarios:

1. Responsable ante la Oficina de Tecnología e Información de la Guardia Nacional de Puerto Rico
 - a. Reconocen la autoridad de OTI de monitorear y controlar los servicios que están disponibles para la agencia y sus usuarios.
 - b. Reconocen que los sistemas de información de las entidades gubernamentales, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico y la Agencia.
 - c. Reconocen que los sistemas de información y las herramientas asociadas, como el correo electrónico y el Internet solo podrán ser utilizados por aquel personal debidamente autorizado, y el uso de tales recursos constituye un *privilegio* otorgado con el propósito de agilizar los trabajos de la entidad gubernamental. Por lo tanto, los usuarios reconocen expresamente que dicho acceso a los sistemas de información no es un derecho.
 - d. Reconocen que la OTI no es responsable del contenido, ni por la gama de información disponible en el Internet a través de los servicios y no edita o manipula la información de ninguna manera que no sea para alcanzar los requerimientos técnicos y operacionales.

BORRADOR

2. Seguridad de Cuentas y Contraseñas

- a. Son responsables por la seguridad de las cuentas y contraseñas asignadas a estos. Cada usuario es responsable de tomar todas las medidas razonables para evitar y prevenir que su cuenta y contraseña sea conocida por alguna otra persona.
- b. Cada usuario es quien único está autorizado a utilizar su cuenta y contraseña.

3. Uso del Sistema de Información y Acuerdo de Usuario

- a. Cada usuario tiene el deber de hacer todos los esfuerzos y medidas razonables para que el uso de los servicios y/o uso del Internet se haga de una manera eficiente y económica.
- b. Cada usuario tiene el deber y obligación de acatar las instrucciones, verbales o escritas, impartidas por el personal de la OTI relacionada al uso de sistemas de información y el Internet.
- c. En la eventualidad que un usuario haya obtenido o enviado inadvertidamente información sin contar con autorización para ello debe informarlo inmediatamente a la OTI o a la gerencia una vez advenga en conocimiento de dicha situación.
- d. Todo usuario debe firmar el Acuerdo de Usuario antes que se le autorice acceso a los servicios y el Internet.

VIII. Normas aplicables al Uso del Internet

Este servicio constituye un privilegio sujeto a las siguientes limitaciones y prohibiciones:

- A. Los servicios de Internet de la Agencia tendrán uso oficial dentro de Puerto Rico, en el área Continental de los Estados Unidos y con países extranjeros con el propósito de establecer contacto con entidades gubernamentales estatales, federales y locales; universidades y colegios; entidades proveedoras de tecnologías, información sobre reglamentos, legislaciones y otros materiales similares.

BORRADOR

- B. Se podrá establecer contacto oficial para propósitos de desarrollo profesional y actualización del conocimiento en el ámbito del campo de especialización del usuario.
- C. Los Sistemas de comunicación y acceso a la Internet son propiedad de la GNPR y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las Normas de Conducta y Medidas Disciplinarias de la Agencia aprobadas el 16 de junio de 2003 y nunca con fines no oficiales o para actividades personales, actividades político-partidistas ni religiosas. o con fines de lucro.
- D. Las operaciones realizadas a través del Internet pueden generar responsabilidad por parte de las entidades gubernamentales del Estado Libre Asociado, por lo que los usuarios que tengan acceso al Internet a través de la Agencia no podrán reclamar interés propietario o expectativa de intimidad sobre comunicaciones utilizando dichos medios.
- E. La Agencia se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso al Internet y el contenido de lo accedido.
- F. La Guardia Nacional, a través de OTI, no se responsabiliza de la validez, calidad, contenido o corrección de la información contenida en el Internet.
- G. La publicación de información de la GNPR a través de la Internet será debidamente autorizada por el Ayudante General o su representante autorizado.

IX. Normas aplicables al Uso de Correo Electrónico.

- A. Los servicios de Correo Electrónico de la Agencia tendrán uso oficial dentro de Puerto Rico, en el área Continental de los Estados Unidos y con países extranjeros con el propósito de establecer contacto con entidades gubernamentales estatales, federales y locales; universidades y colegios; entidades proveedoras de tecnologías, información sobre reglamentos, legislaciones y otros materiales similares.
- B. Se podrá establecer contacto oficial para propósitos de desarrollo profesional y actualización del conocimiento en el ámbito del campo de especialización del usuario.

BORRADOR

- C. El sistema de Correo Electrónico es propiedad de la Agencia y es parte integral de sus sistemas de información, por lo que la misma se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo, por lo que los usuarios no podrán reclamar interés propietario o expectativa de intimidad sobre comunicaciones.
- D. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro, actividades político-partidistas ni religiosas o con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados.
- E. El personal que utilicen el sistema de Correo Electrónico deberán velar por el cumplimiento de las normas aplicables al comportamiento de los usuarios autorizado por la entidad al momento del uso de este sistema.
- F. Toda comunicación electrónica que se reciba, emita o archive deberá salvaguardar en todo momento el buen nombre y la responsabilidad de la Agencia y sus organismos adscritos.
- G. Se prohíbe el envío de copias de mensajes de correspondencia electrónica con información confidencial sin el consentimiento del remitente original.

X. Política Sobre Privacidad

- A. La GNPR tomará las medidas razonables para proteger la confidencialidad y privacidad de la información personal guardada en los sistemas o que pase a los archivos mediante el uso por parte del usuario de los servicios de comunicación existentes y los que se implanten en el futuro. No se revelará, divulgará o compartirá datos personales o confidenciales del personal con otro organismo o persona excepto:
 - 1. Para cumplir con n requerimiento judicial
 - 2. En situaciones de riesgo de daño físico o amenaza de peligro para un usuario, a Agencia o terceras personas
 - 3. Cuando sea necesario para prevenir o detener intento de vulnerar la seguridad del Sistema o de alguno de sus componentes
 - 4. Cuando se trate de una situación que involucre la comisión de un delito.

BORRADOR

B. Los funcionarios y empleados autorizados a utilizar los sistemas de información recibirá copia de este Reglamento. Una vez firmado el recibo, el usuario aceptará que los servicios electrónicos y las comunicaciones electrónicas hechas a través del Sistema son propiedad de la GNPR y que cumplirá con las condiciones, limitaciones y prohibiciones en el uso del Sistema y sus Servicios, así como las establecidas por la Agencia.

C. Al acceder los Sistemas aparece un mensaje de la Agencia al usuario reiterando el acuerdo de que el uso autorizado es para propósitos oficiales y confirmando la política de la Agencia.

D. No se reconocerá un derecho o una expectativa de intimidad en cuanto a los documentos y los mensajes creados, enviados o recibidos mediante el uso del Sistema. La GNPR no puede garantizar la privacidad y confidencialidad de la información no oficial que el usuario provea a través de los sistemas de comunicación.

E. Las gestiones personales del usuario no deberán ser atendidas como asunto rutinario mediante el uso del Sistema. No obstante, no constituirá conducta sancionable el que el usuario ocasional o esporádicamente utilice el sistema para gestiones personales fuera de horas laborables y cuando así hacerlo:

1. no se violenten otras disposiciones legales o reglamentarias pertinentes, incluyendo lo dispuesto en este Reglamento;
2. no se afecte adversamente el desempeño de las funciones oficiales del usuario, su productividad y eficiencia en el trabajo, o su cumplimiento con el horario de trabajo requerido;
3. no se afecte adversamente la imagen de la Agencia;
4. no se afecte la capacidad del sistema para procesar la información mediante, como ejemplo, comunicaciones en masa, SPAM o el almacenamiento de archivos de tamaño excesivo.
5. No se lleven a cabo gestiones con fines de lucro.

BORRADOR

Todas las comunicaciones efectuadas en estas circunstancias estarán sujetas a las normas, limitaciones y prohibiciones establecidas en este Reglamento. Por consiguiente, si el empleado o funcionario opta por atenderlas mediante las computadoras y equipo electrónico de la Agencia, el contenido de sus mensajes pasará a los archivos del Sistema y estará sujeto a los derechos y prerrogativas de la GNPR, quien se reserva, sin necesidad de notificación previa al empleado o funcionario.

El usuario, no deberá usar los Sistemas de comunicación electrónica de la Agencia cuando el tercero con quien se comunica no desea que los mensajes sean leídos o divulgados por la Agencia, y no podrá albergar una expectativa irrazonable de intimidad, según establecido por las disposiciones legales.

XI. Política Antidiscrimen

El correo electrónico y el Internet no se utilizarán en forma que resulte ofensiva o discriminatoria en forma alguna respecto a los empleados y visitantes, o que pueda provocar incomodidad o despertar reacciones emocionales indeseadas en la persona que reciba la comunicación.

Se prohíbe el uso de la computadora o correo electrónico para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razones de raza, genero, credo, ideas políticas u origen social o nacional así como opiniones sobre personas con impedimento físico o mental.

Se prohíbe el envío de mensajes, materiales o imágenes de contenido difamatorio, falso, abusivo, obsceno, pornográfico, amenazante o en cualquier forma ilegal que afecte la imagen de la GNPR. Esto incluye, acceso a material erótico, bromas de cualquier forma o comentario o chiste que pueda violar la política antidiscrimen y Hostigamiento Sexual de la GNPR.

XII. El Servicio de los Sistemas de Información

Códigos de Acceso y Auditoria de los Sistemas

La asignación de códigos de acceso no impedirá que el uso de los sistemas de información sea auditado por el personal autorizado por la Agencia a tales fines, con el propósito de garantizar el uso apropiado de los recursos de la entidad gubernamental.

Expectativa de Intimidad

Los usuarios, **no tienen** expectativa de intimidad alguna con relación a la información almacenada en su computadora o que sea emitida o

BORRADOR

comunicada a través de los sistemas de información del Estado Libre Asociado de Puerto Rico.

Información con Carácter de Documentos Públicos

Los documentos generados o contenidos en los sistemas de información de la Agencia son parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

La información desarrollada, transmitida o almacenada en los sistemas de información es propiedad de la Agencia y del Estado Libre Asociado de Puerto Rico, por lo que le aplican todas las disposiciones legales relacionadas a los documentos públicos.

XIII. Uso No Autorizado

Los Usuarios de los Sistemas de Información no están permitidos a incidir en la siguiente conducta:

- A. Divulgar o compartir la contraseña (Password).
- B. Copiar, divulgar, transferir, examinar, cambiar o borrar información o programas que le pertenecen a otro usuario sin la expresa autorización de éste o de OTI.
- C. Copiar, divulgar, transferir, examinar, cambiar o borrar información o programas que le pertenecen al Estado Libre Asociado de Puerto Rico y/o la Agencia sin la expresa autorización de la gerencia o de OTI.
- D. Interferir con las operaciones del Servicio.
- E. Interferir con el servicio de Internet del Estado Libre Asociado de Puerto Rico y/o de la Agencia.
- F. Evadir cualquier restricción y/o seguridad impuesta para el uso de los servicios y el Internet.
- G. Utilización de protectores de monitores (Screen Savers) con fotos, imágenes o mensajes cuyo contenido pueda resultar ofensivo o incida en conducta prohibida.
- H. Uso de los sistemas de información o el Internet para obtener acceso no autorizado a cualquier otra facilidad de computadoras o servicio de sistemas de información.

BORRADOR

- I. Copiar cualquier otro programa, data o información sin la previa autorización del dueño de los derechos de autor o de la Agencia.
- J. Enviar cualquier material por el Internet que identifique al usuario y proyecte la Agencia de manera que afecte la imagen y el nombre de esta.
- K. Utilizar los servicios y/o el Internet para crear falsas representaciones, proveer datos ficticios o anónimos.
- L. Intentar descubrir las cuentas y/o contraseñas de otros usuarios, o para esos servicios que el acceso apropiado no haya sido autorizado para ese usuario.
- M. Ejecutar cualquier acción mediante la utilización del Internet que constituya conducta inaceptable.
- N. Iniciar o continuar correos electrónicos en cadena.
- O. Utilizar el correo electrónico para beneficio personal.
- P. Utilizar durante horas laborables cuentas de correo electrónico distintas a las provistas por la Agencia, sin el debido consentimiento de la OTI.
- Q. Enviar o recibir correos electrónicos y sus anejos cuya capacidad de memoria excede los 2 Mega Bytes (2MB).
- R. Enviar o recibir correos electrónicos personales a su cuenta de correos electrónicos provista por la Agencia.
- S. Enviar o recibir correos electrónicos sin que el contenido y sus recipientes estén autorizados por la agencia a recibir o enviar correos electrónicos dentro del sistema de servicios de información.
- T. Acceder y abrir correos electrónicos provenientes del Internet sin llevar a cabo un rastreo de virus.
- U. Acceder y abrir archivos solicitados y no solicitados recibidos del Internet sin realizar un rastreo de virus.
- V. Instalar programas en cualquier equipo de los sistemas de Información para los cuales no exista una licencia o autorización válida a nombre de la Agencia.

BORRADOR

comunicada a través de los sistemas de información del Estado Libre Asociado de Puerto Rico.

Información con Carácter de Documentos Públicos

Los documentos generados o contenidos en los sistemas de información de la Agencia son parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

La información desarrollada, transmitida o almacenada en los sistemas de información es propiedad de la Agencia y del Estado Libre Asociado de Puerto Rico, por lo que le aplican todas las disposiciones legales relacionadas a los documentos públicos.

XIII. Uso No Autorizado

Los Usuarios de los Sistemas de Información no están permitidos a incidir en la siguiente conducta:

- A. Divulgar o compartir la contraseña (Password).
- B. Copiar, divulgar, transferir, examinar, cambiar o borrar información o programas que le pertenecen a otro usuario sin la expresa autorización de éste o de OTI.
- C. Copiar, divulgar, transferir, examinar, cambiar o borrar información o programas que le pertenecen al Estado Libre Asociado de Puerto Rico y/o la Agencia sin la expresa autorización de la gerencia o de OTI.
- D. Interferir con las operaciones del Servicio.
- E. Interferir con el servicio de Internet del Estado Libre Asociado de Puerto Rico y/o de la Agencia.
- F. Evadir cualquier restricción y/o seguridad impuesta para el uso de los servicios y el Internet.
- G. Utilización de protectores de monitores (Screen Savers) con fotos, imágenes o mensajes cuyo contenido pueda resultar ofensivo o incida en conducta prohibida.
- H. Uso de los sistemas de información o el Internet para obtener acceso no autorizado a cualquier otra facilidad de computadoras o servicio de sistemas de información.

BORRADOR

- W. Está prohibido participar en los programas de charlas "chats", excepto cuando se refieren a usos relacionados con las responsabilidades de la Agencia.

XIV. Normas relacionadas a la Seguridad

Con el propósito de proteger y garantizar la seguridad del Sistema y su utilización para fines autorizados, se adoptan las siguientes normas:

- A. El uso de un código de acceso ("password"), no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra. Las contraseñas deben mantenerse en estricta confidencialidad y administrarse conforme al Memorando sobre medidas de seguridad adoptadas por la GNPR. Al aceptar utilizar esta computadora usted reconoce haber leído y entendido dicho Memorando.
- B. Cada usuario adoptará una contraseña secreta de acceso al sistema la cual cambiará y validará cada 90 días. El usuario será responsable de proteger la confidencialidad de su contraseña. No deberá revelarlos, compartirlo, dejarlo accesible a otras personas o incluirlos en documentos o archivos.
- C. La GNPR se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la GNPR no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de "e-mail".
- D. Para evitar poner en peligro la confidencialidad de la información de la GNPR, se prohíbe el envío fuera de la misma de documentos electrónicos o mensajes por medio del "e-mail" que contengan información privilegiada o confidencial.
- E. Se prohíbe el envío o recibo de mensajes de correo electrónico entre el personal de la GNPR y otras personas que no pertenezcan a la Organización, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, religión, personas o cualquier otra situación o asunto interno de la GNPR.

BORRADOR

que puedan poner en entredicho la reputación o imagen de la Agencia, aunque la información divulgada no sea de naturaleza confidencial.

- F. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.
- G. Se prohíbe terminantemente codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la GNPR con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivos. En el caso de que por razones de seguridad, el Oficial Principal de Informática, permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la GNPR estará facultada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo.
- H. Se prohíbe la modificación de los parámetros o configuración de las computadoras de la GNPR para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la Agencia.
- I. Se prohíbe el uso de discos magnéticos o cualquier otro medio de almacenaje de información, sin que haya sido verificado o certificado como libre de virus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.
- J. Todos los archivos que se creen en las computadoras deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo (backup) existentes.

XV. Infracciones

Infracciones a este Reglamento darán base para iniciar un proceso administrativo de conformidad con el Manual de Normas de Conducta y Medidas Disciplinarias de la Agencia aprobado el 16 de junio de 2003. En casos donde el infractor sea un Contratista, podría resultar en la revocación inmediata del contrato.

BORRADOR

XVI. Cláusula de Separabilidad

Si cualquier cláusula o disposición de este Reglamento fuere declarada ilegal o inconstitucional por un Tribunal de Justicia con jurisdicción y competencia, por sentencia final y firme, tal declaración no afectará la validez de las demás cláusulas, las que mantendrán su validez y efecto y la declaración de nulidad o invalidez quedará limitada al artículo, sección o inciso objeto de la misma.

XVII. Vigencia

Este Reglamento entra en vigor inmediatamente. La Oficina de Recursos Humanos notificará individualmente a cada usuario de la Agencia con copia del presente Reglamento. El empleado deberá certificar con su firma el acuse de Recibo.

Aprobado en San Juan, Puerto Rico hoy de de 2010

Antonio J. Vicéns
General de División, (PR), GNPR
Ayudante General

Revisado por: _____
Lcdo. Francisco De Jesús
Asesor Legal

Fecha: _____

BORRADOR

GUARDIA NACIONAL DE PUERTO RICO

DIV. SERVICIOS ADMINISTRATIVOS

OFICINA DE INFORMATICA

PLAN DE CONTINUIDAD OPERACIONAL

GUARDIA NACIONAL DE PUERTO RICO

OFICINA DE INFORMATICA

(DIV. SERVICIOS ADMINISTRATIVOS)

PLAN DE CONTINUIDAD OPERACIONAL

Tabla de Contenido

A. Propósito.....	1
B. Localización de la Oficina de Informática.....	1
C. Medidas de Control a Tomarse en consideración en la Oficina de Informática en caso de que ocurra una emergencia y/o desastre.....	1
D. Responsabilidades del Personal de la Oficina.....	1-2
E. Responsabilidades del Grupo Técnico de la Oficina de Informática.....	2
F. Medidas de Control y Seguridad en Casos de Emergencia.....	2-3
G. Medidas de Recuperación Después de un Caso de Emergencia.....	4
H. Guías para Resguardo.....	4
I. Grupos de Recuperación.....	4
J. Itinerario de Restauración.....	4-5
K. Aplicaciones.....	5
L. Configuración de Programas.....	5
M. Inventario de Equipo.....	5-6
N. Dependencias Estatales en Caso de Emergencia y/o Desastres.....	6

BORRADOR

GUARDIA NACIONAL DE PUERTO RICO

OFICINA DE INFORMATICA

(DIV. SERVICIOS ADMINISTRATIVOS)

A. PROPÓSITO

El procedimiento descrito a continuación ha sido diseñado con el propósito de establecer las medidas de seguridad necesarias para proteger el personal, equipo y/o propiedad de la Oficina de Informática en caso de incendios, desastres naturales como terremotos, huracanes y otros, además de orientar a todo el personal de manera que actúe con serenidad en caso de que ocurra una de las mencionadas emergencias.

Este plan permitirá establecer y mantener en funcionamiento la Oficina de Informática de manera que oriente y capacite al personal para enfrentarse a situaciones de emergencia. Además, especificará los deberes y responsabilidades de cada empleado de manera que puedan tomar medidas preventivas para la conservación y seguridad de la planta física, propiedad, equipo, etc., así como hacer las asignaciones correspondientes durante la emergencia.

B. LOCALIZACIÓN DE LA OFICINA DE INFORMÁTICA

La Oficina de Informática de la Guardia Nacional de Puerto Rico está localizada en la Calle General Esteves, Parada 3 1/2, Puerta de Tierra, San Juan, PR 00902. División de Servicios Administrativos, Teléfono (787)721-3131 (Ext.7038, 7039,7001.

C. MEDIDAS DE CONTROL A TOMARSE EN CONSIDERACION EN LA OFICINA DE INFORMÁTICA EN CASO DE QUE OCURRA UNA EMERGENCIA Y/O DESASTRE:

La Oficina de Informática de GNPR ha establecido un plan de resguardo el cual tiene como propósito identificar los pasos y medidas necesarias para salvaguardar los activos y garantizar el restablecimiento de las operaciones de la oficina.

En este plan se establecen las responsabilidades de la Oficina de Informática para la obtención y almacenamiento de la información, además, incluye la frecuencia del proceso e itinerarios de resguardos.

Su objetivo es proveer una guía para mantener la integridad del sistema de información de la GNPR, además de asegurar el restablecimiento de los procesos en aquellos casos donde el computador principal o las facilidades donde se ubica este queden inoperantes. Su alcance es identificar archivos corrientes que se deben salvaguardar y su frecuencia de resguardo. Establece también las responsabilidades por función, documentación actualizada y mantenimiento necesario para darle continuidad y mantener el plan efectivo a través del tiempo; independientemente de cambios y/o crecimiento de la oficina.

D. RESPONSABILIDADES DEL PERSONAL DE LA OFICINA PARA LA PROTECCIÓN Y SEGURIDAD DEL EQUIPO DE INFORMÁTICA

1. El empleado que se encuentre en su área de trabajo deberá velar lo siguiente:
 - Cerrar todos los archivos en los cuales está trabajando; remover y guardar los discos.
 - Apagar todos los sistemas a su cargo.
 - Apagar la impresora o cualquier otro equipo en el área.
 - Desconectar todos los equipos de las tomas eléctricas.
 - Cubrir los equipos con bolsas plásticas para protegerlos de humedad.
 - Retirar cualquier equipo que esté cerca de una ventana.

BORRADOR

2. Al finalizar la emergencia, realizar inventario tanto del equipo como del área de trabajo y verificar la toma eléctrica que esté en buenas condiciones de lo contrario, deberá informar el desperfecto a la División de Ingeniería. Luego deberá asegurarse de que:
 - Ninguna de las bolsas plásticas de los equipos estén húmedas.
 - El monitor no tenga rota la pantalla.
 - La impresora esté en buenas condiciones.
 - De encontrar algún equipo roto, no intente operarlo.
3. De existir algún problema en lo antes expuesto, prepare un informe de daños el cual debe contar con lo siguiente:
 - Su nombre, fecha, hora.
 - Sección para la cual trabaja, número de estación y número de extensión.
 - Descripción del equipo que considera dañado.
 - Detalle en forma breve lo que se entienda le pasó al equipo.
4. Terminado el informe entregarlo al administrador de la red.

E. RESPONSABILIDADES DEL GRUPO TÉCNICO DE LA OFICINA DE INFORMÁTICA

El personal técnico de la Oficina de Informática será responsable de:

1. Mantenerse en constante comunicación con la oficina (antes, durante y después de la emergencia).
2. Estar a disposición el tiempo necesario en que se necesiten sus servicios.
3. Tomar las medidas de seguridad y precauciones necesarias para que no afecten su seguridad personal.
4. Proveer forma o manera de cómo localizarle.

F. MEDIDAS DE CONTROL Y DE SEGURIDAD EN CASOS DE EMERGENCIA

1. AVISO DE EXPLOSIVOS

- La persona que reciba la llamada deberá anotar la hora exacta en que se recibió la misma.
- Notificar inmediatamente vía telefónica al Cuerpo de Bomberos y a la Policía de Puerto Rico.
- Cuando se notifica al personal que está bajo una alarma de explosivos, el mismo deberá de permanecer en su área hasta tanto se reciban ordenes de abandonar la oficina.
- Es importante familiarizar al personal con los medios de salida del edificio y/u oficina y cómo usarlos de manera segura y eficiente. El orden y control son los factores más importantes a observarse, a los fines no solamente de evitar accidentes sino evitar caer en estado de pánico y como consecuencia, la pérdida de vidas.
- Utilizar las escaleras y el desalojo en forma ordenada y cuidadosa, haciendo uso de los pasamanos para evitar accidentes.
- No se permitirá el movimiento de personas en dirección contraria.
- Las puertas con libre acceso estarán rotuladas con la frase "EXIT" o "SALIDA".
- Todo el personal obedecerá las ordenes emitidas por las personas autorizadas y seguirán las rutas de desalojo establecidas.

BORRADOR

2. MEDIDAS DE DESALOJO EN CASO DE INCENDIO

- Todo el personal deberá adiestrarse en la manera de cómo utilizar los extintores.
- Cada empleado deberá conocer la localización de los extintores.
- Los extintores se colocarán en lugares visibles y accesibles.
- La primera persona que detecte un incendio deberá dar alerta inmediatamente, y si le es posible, comunicarse vía telefónica con el Cuerpo de Bomberos. Además, deberá en la medida que sea posible, intentar apagar el fuego haciendo uso de los extintores y tomando las debidas precauciones.

3. MEDIDAS DE SEGURIDAD EN CASO DE UN FENOMENO ATMOSFÉRICO

- Sintonizar la radio o televisor para escuchar los informes emitidos por el Servicio Nacional de Meteorología así como cualquier otra información y asesoramiento que pueda ser emitido o radiodifundido por el gobierno local.
- Planificar el tiempo debidamente y realizar los preparativos para evitar los inconvenientes antes de que llegue el fenómeno atmosférico.
- Si ocurre durante fin de semana o día feriado, estar atento para determinar el día que se asistirá a la oficina para dejar en un lugar seguro los objetos sueltos que haya dentro de la oficina tales como: máquinas, tiestos, escritorios, zafacones, etc.
- Siempre se debe mantener la calma, no prestar atención a rumores.
- No hacer llamadas telefónicas innecesarias.
- Almacenar en un lugar seguro los objetos sueltos que haya dentro de la oficina tales como: máquinas, tiestos, escritorios, zafacones, etc.
- Tomar precauciones con el uso de linternas, lámparas o velas, para evitar incendios.
- La succión creada por la diferencia en la presión atmosférica dentro y fuera de la oficina puede destruir ventanas o puertas. Para evitar esto abra una ventana o puerta en el lado opuesto a la dirección que normalmente sopla el viento.
- Pasado el fenómeno atmosférico, no toque ninguna línea eléctrica. Informe, si es posible, a la Autoridad de Energía Eléctrica, Defensa Civil o el Cuerpo de Bomberos.

4. MOVIMIENTOS TELURICOS (SISMOS/TERREMOTOS)

- Si el terremoto o sismo ocurre estando usted dentro de la oficina, manténgase adentro. Si puede, llegue hasta el área de las escaleras, no utilice los ascensores. Proteja su vida bajo un escritorio, una mesa, bajo el marco de una puerta, en los pasillos o contra las paredes interiores. Manténgase lejos de cristales y puertas que dan al exterior.
- No utilice velas, fósforos u otros objetos inflamables ya sea durante o después del sismo. Apague, en la medida que sea posible y si tiene las facilidades y/o equipo, cualquier incendio que se haya originado.
- Si el terremoto ocurre estando fuera del edificio donde está ubicada la oficina, evite el contacto con cables eléctricos hasta que el sismo termine.
- No corra cerca o entre a edificios, uno de los mayores peligros radica en la caída de pedazos de vidrio o bloques de niveles altos.
- Si se encuentra en un vehículo de motor cuando sucede el sismo, detenga el mismo tan pronto la sea posible de manera que no ocasione accidentes.

BORRADOR

8	B	Notificar a los diferentes suplidores de equipo y otros productos sobre la emergencia y alertarlos sobre las posibles necesidades.
9	C	Activar el Grupo de Restauración.
10	B	Activar el Grupo Operacional.
11	C	Identificar y relocalizar equipo, archivos e inventario. Relocalizar respaldos de bóvedas externas al Centro Alternativo.
12	B,C	Reunirse con suplidores e identificar necesidades para la restauración.
13	A,C	Iniciar restauración de utilidades generales y seguridad.
14	C	Restaurar la data, programas, y las telecomunicaciones.
15	C	Reconstruir el medio ambiente de producción.
16	A,B,C	Revisar tiempo de restauración e itinerarios.
17	C	Conducir pruebas de los sistemas y verificar operaciones del Centro Primario.
18	A,B	Notificar a todos los miembros de grupos, clientes y suplidores sobre la relocalización al Centro Primario.
19	C	Reconstruir archivos de producción y librerías.
20	C	Relocalizar el procesamiento de programas y archivos de producción al Centro Primario.
21	C	Revisar el procesamiento y buen funcionamiento de todas las aplicaciones.
22	C	Relocalizar todo el inventario y discontinuar el uso y accesos al Centro Alternativo. Crear respaldos de archivos críticos de sistema y producción.
23	A,B,C	Evaluar el evento y actualizar el Plan de Continuidad de Negocio.

K. APLICACIONES

<u>APLICACIÓN</u>	<u>PERSONA RESPONSABLE</u>	<u>CLASIFICACIÓN</u>
Microsoft Exchange	Director(a) de Informática	Indirecta
PRIFAS y RHUM Kronos WFC 6.0	Director(a) de Finanzas Director de Rec. Hum. y Director(a) de Informática	Interna Externa
MIP Accounting Microix	Director(a) de Finanzas y Director(a) de Informática	Interna Externa

La tarea para restaurar estas aplicaciones es localizar el resguardo más reciente y restaurarlo en el Centro Alternativo.

L. CONFIGURACIÓN DE PROGRAMAS

La configuración de los sistemas operativos utilizados en la GNPR, es Windows XP SP3 en las estaciones de trabajo y Windows Server 2003 SP1 en los servidores.

M. INVENTARIO DE EQUIPO

El propósito de esta sección es proveer un detalle de toda la configuración de los sistemas (equipo) del Centro Primario.

- Inventario del Equipo del Centro de Datos Primario:

<u>MARCA</u>	<u>MODELO</u>	<u>SERVIDOR</u>	<u>SISTEMA OPERATIVO</u>	<u>USO</u>
HP	Dell Power Edge 2600	GNPR Exchange_01	Windows Server 2003 SP1	Active Directory, PDC Emulator, DHCP, DNS,IIS,WINS Email Server

BORRADOR

HP	Proliant ML350	GNPR-Firewall-isa	Windows Server 2003 SP1	ISA Firewall, Backup Server
HP	Dell Power Edge 2400	GNPR-Fil-Prt-01	Windows Server 2003 SP1	Active Directory, DNS, DHCP, WINS, File Print Server
HP	Storage Works AiO400	GNPR-san	Windows Storage Server 2003 SP1	WSUS, PRIFAS RHUM File Server, ISCSI Hosting, Doculex Web Server
HP	Dell Power Edge 2600	GNPR-Db-01	Windows Storage Server 2003 SP1	Data Base Server SQL SERVER MIP, MICROIX
HP	Proliant ML 359 G-6	GNPR-Kronos-Db	Windows Server 2003 SP2	Data Base Server SQL SERVER Kronos WFC 6.0
HP	Proliant ML 359 G-6	GNPR-Kronos-Tel	Windows Server 2003 SP2	Kronos Tele Time

El equipo necesario para cumplir con el proceso de restauración es el siguiente:

<u>SISTEMA OPERATIVO</u>	<u>PROCESSOR</u>	<u>RAM</u>	<u>HDD</u>	<u>USO</u>
Windows Server 2008	Intel Xeon E5530	4GB	500GB	Active Directory, ISA Firewall, Web Server, Backup Server, WSUS, MIP, MICROIX
Windows Server 2008 (utilizando virtualización)	2x Intel Xeon E5530	16GB	1TB	Active Directory, PDC Emulator, DHCP, DNS, Email, File, Print Server
Windows Server 2008	Intel Xeon E5530	8GB	500GB	Kronos WFC 6.0 y Tele Time, SQL

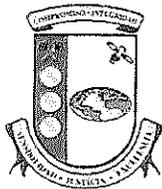
N. DEPENDENCIAS ESTATALES EN CASO DE EMERGENCIAS Y/O DESASTRES

<u>Agencia</u>	<u>Teléfono</u>
Cuerpo de Bomberos	(787) 343-2330
Cuerpo de Emergencias Médicas	(787) 775-0550
Policía de Puerto Rico	(787) 343-2020
Manejo de Emergencias (AEMEAD)	(787) 724-0124
Servicio Nacional de Meteorología	(787) 253-4586
Cruz Roja Americana	(787) 729-9400

Aprobado por: _____

Fecha: _____

BORRADOR



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

3 de febrero de 2011

vortiz@gnpr.gobierno.pr

Gen. Ret. Antonio J. Vicens González
Ayudante General
Guardia Nacional
San Juan, Puerto Rico

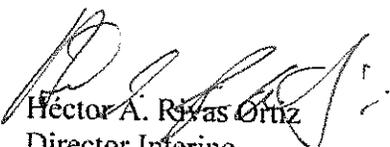
Estimado general Vicens González:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-5)* que nos remitió el 2 de febrero de 2011, relacionado con el *Informe de Auditoría DA-09-03* de la Guardia Nacional de Puerto Rico. Determinamos que las **recomendaciones 1 y 5.b.2)** se consideran cumplimentadas.

Para información adicional, el funcionario designado por usted puede comunicarse con el Sr. Pedro J. Collado León, Analista del Plan de Acción Correctiva, al (787) 294-1991, extensión 518.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,


Héctor A. Rivas Ortiz
Director Interino
División "A" de Auditorías
de Departamentos y Agencias

c Hon. Carlos J. Torres Torres
Presidente
Comisión Conjunta sobre
Informes Especiales del Contralor

Sr. Víctor M. Ortiz
Oficial Ejecutivo para Asuntos Estatales
Guardia Nacional de Puerto Rico

PO BOX 366069 SAN JUAN, PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gou.pr INTERNET: <http://www.ocpr.gou.pr>



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: DA-09-03 Número de unidad: 1422 Entidad auditada: Guardia Nacional de Puerto Rico

Fecha del informe: 11 de agosto de 2008 Período auditado: 1 de julio de 1999 al 30 de junio de 2006

Índice: PAC ICP - 5

Funcionario enlace: Victor M. Ortiz, Coronel (Ret) Puesto: Oficial Ejecutivo para Asuntos Estatales Teléfono: (787) 721-3131 Ext. 7000

Funcionario principal o su representante autorizado: General Antonio J. Vicéns Puesto: Ayudante General Teléfono: (787) 721-3131 Ext. 1631
Antonio J. Vicéns Fecha: 31 de enero de 2011

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA *Antonio J. Vicéns*
 Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
1. Evidencia de la aprobación del Reglamento del Uso y Manejo de los Recursos de Informática. Hallazgo 5-a.1.	Establecimos el Reglamento Sobre el Uso y Manejo de los Sistemas de Información y Tecnología de la Guardia Nacional de Puerto Rico.	Cumplimentado. El Reglamento Sobre el Uso Y Manejo de los Sistemas de Información y Tecnología de la Guardia Nacional de Puerto Rico esta aprobado por el Ayudante General desde el 27 de enero de 2011 y se implantará inmediatamente. (Ver anejo).
2. Evidencia de la aprobación del Ayudante General de un Plan de Contingencias que incluya las medidas a considerar para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información en caso de ocurrir algún desastre o circunstancia que afecte las operaciones normales de la entidad. Hallazgo 5-a.3	Se aprobó Plan de Continuidad Operacional con las medidas de control a tomarse cumpliendo con las necesidades En casos de emergencia, desastre, fuego o cualquier circunstancia que afecten las operaciones normales en la Agencia.	Cumplimentado. El Plan de Continuidad Operacional esta aprobado desde el 27 de enero de 2011 y se implantará inmediatamente. Además, se implantarán las Normas sobre el Uso de los Sistemas Electrónicos. (Ver Anejo).

(Véase instrucciones al final del modelo)

**GUARDIA NACIONAL DE PUERTO RICO
DIVISIÓN DE SERVICIOS ADMINISTRATIVOS
OFICINA DE INFORMÁTICA**

**REGLAMENTO SOBRE EL USO DE SISTEMAS
DE TECNOLOGÍA E INFORMACIÓN**

REGLAMENTO SOBRE EL USO DE LOS SISTEMAS DE TECNOLOGÍA E INFORMACION DE
LA GUARDIA NACIONAL DE PUERTO RICO

I. Base Legal

Este Reglamento se establece de conformidad con las disposiciones de la Ley número 62 del 23 de junio de 1969, según enmendada, conocida como el Código Militar de Puerto Rico y la Ley Núm. 151 de 22 de junio de 2004, según enmendada.

II. Política Pública

La Ley Núm. 151 del 22 de junio de 2004, adopta como uno de sus elementos principales la creación de una serie de normas que garanticen el uso adecuado, efectivo y seguro de los sistemas de tecnología e información del gobierno de Puerto Rico. Dichas normas deben ser orientadas a la obtención de logros y a fomentar activamente la innovación para mejorar y agilizar los procesos de la Guardia Nacional de Puerto Rico.

III. Propósito

Este reglamento tiene el propósito de cumplir con la política pública de establecer las medidas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de tecnología e información.

IV. Alcance

El presente reglamento establece el conjunto de normas y medidas correspondientes para proporcionar a los usuarios de la Guardia Nacional de Puerto Rico acceso a los sistemas de tecnología, información, comunicación, Internet y uso de Correo Electrónico del Gobierno de Puerto Rico.

De igual manera, este reglamento crea las condiciones necesarias para garantizar que el uso de los sistemas de tecnología e información gubernamental y sus aplicaciones se haga de una forma segura, efectiva y adecuada.

Este documento define y detalla el uso aceptable de la información que se maneja a través de los sistemas de información del gobierno. El mismo tiene la intención de proteger al usuario, a la Guardia Nacional de Puerto Rico y al Gobierno de Puerto Rico mediante proscripción de aquella conducta que ponga en riesgo los sistemas y la información que estos contienen.

V. Definiciones

- A. Acuerdo- Entiéndase Acuerdo del Usuario según establecido en este Reglamento.
- B. Agencia- Para propósitos de este reglamento se entenderá como agencia – la Guardia Nacional de Puerto Rico.
- C. Antivirus- Programa que protege los sistemas de información de los ataques de virus conocidos.
- D. Cifrar (Encrypt)- Proceso en el cual los datos se convierten a un formato que no puede descifrarse fácilmente por personas no autorizadas a acceder los mismos.
- E. Contraseña (Password)- Secuencia de caracteres que se utiliza para comprobar que el usuario que está requiriendo acceso a un sistema o programa es realmente ese usuario.
- F. Oficial Principal- Entiéndase Oficial Principal de Informática (OPI) de la Guardia Nacional de Puerto Rico.
- G. OTI- Entiéndase la Oficina de Tecnología e Información de la Guardia Nacional de Puerto Rico.
- H. DCSIM- Directorado de Informática Federal.
- I. Usuario- Entiéndase, funcionario, empleado, contratista y personal militar que se le ha concedido acceso a los sistemas de información de la Guardia Nacional de Puerto Rico.

J. Servicio- Entiéndase aquellos servicios de Sistemas de Información tales como:

1. La utilización de programas de oficina
2. Correo Electrónico
3. Uso de impresoras, fotocopiadoras y fax
4. Computadoras y sus periferales
5. Servidores
6. Bases de datos
7. Telecomunicaciones
8. Otros dispositivos conectados a la red de computadoras de la Agencia, el Internet y aquellos otros que resulten en una red de computadoras y datos donde existen dichos servicios de información que estarán disponibles a aquellos usuarios debidamente autorizados.

K. Servidor- Entiéndase aquella computadora en donde residen y se instalan programas y almacenan documentos que utilizarán otras computadoras.

VI. Responsabilidades

1. Oficina de Tecnología e Información (OTI):

A. Proveer a los usuarios autorizados el acceso apropiado y la configuración de seguridad, luego que cada usuario haya firmado el acuerdo que se encuentra anejado en el presente Reglamento.

B. Configuraré el control de acceso, la seguridad, "Firewall" y todas las aplicaciones de Internet.

C. De detectar que la información enviada o recibida por algún usuario cause o tenga la capacidad de causar daño al Estado Libre Asociado de Puerto Rico o a la Agencia, o esté prohibida por ley o reglamento, OTI está facultado para alterar, remover o grabar dicha información. Una vez ocurra esto, OTI recopilará toda la evidencia disponible y la referirá al

supervisor de dicho usuario para su evaluación. De determinarse que existe una infracción a este Reglamento el supervisor enviará este asunto a la Oficina de Recursos Humanos para el inicio de la acción administrativa correspondiente.

D. Velar por la realización diaria de los resguardos (Backups) de la información contenida en los servidores.

E. Desarrollar e implementar un plan de contingencia, recuperación y/o redundancia en caso de emergencias para mantener la operación de los sistemas de información y telecomunicaciones de la agencia o el restablecimiento de sistemas y datos en caso de desastre en el menor tiempo posible.

F. Garantizar la interoperabilidad de los sistemas de información y comunicaciones de la agencia con otras agencias del Gobierno de Puerto Rico.

G. Establecer un plan para la actualización (update) y modernización (upgrade) de los sistemas de información tanto a nivel de "hardware" y las aplicaciones para garantizar la maximización de los recursos y mejorar la seguridad.

H. Evaluar y recomendar el uso de sistemas de información y comunicaciones que contribuyan a mejorar la producción, reducir gastos operacionales, optimizar servicios y procedimientos o que contribuya con la implementación de una agencia verde de acuerdo a la iniciativa Puerto Rico: Isla Verde.

I. Servir de enlace con la Oficina del DCSIM.

J. Establecer, configurar y mantener las políticas de seguridad para los dominios de la agencia y accesos a la red a través de "Virtual Private Network" (VPN).

K. Proveer asistencia técnica a los usuarios y oficinas de la agencia.

L. Velar que la página de Internet de la Agencia cumpla con los requisitos establecidos por la Oficina de Gerencia y Presupuesto (OGP).

M. Identificar y recomendar aquellos adiestramientos necesarios para que el personal pueda desarrollar y/o reforzar las destrezas necesarias para aumentar la producción y , la maximización de los diversos recursos de los sistemas de información de la agencia.

N. Desarrollar, promover, colaborar, gestionar y dirigir proyectos de tecnología que propendan a un mejor funcionamiento y a la ampliación de servicios de la agencia.

O. Servir de enlace y velar por el cumplimiento de las instrucciones, cartas circulares y cualquier otra reglamentación relacionada con los sistemas de información según establecidos por la Oficina de Gerencia y Presupuesto (OGP).

P. Preparar el Plan Anual de Administración de Recursos Tecnológicos (PAART) exponiendo la estrategia a seguir en el área tecnológica de acuerdo a la visión y misión de la agencia y que a la vez esté orientado al desarrollo de un gobierno electrónico conforme a la TIG-001 y 006 de la OGP.

Q. Mantener un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos clasificados de acuerdo al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad conforme a la TIG-003 de la OGP

R. Redactar, documentar y actualizar constantemente la línea de base (Baseline) de la red de la agencia.

2. Supervisores:

A. Seleccionarán los usuarios y recomendarán los accesos apropiados y la seguridad requerida por ellos.

B. Supervisará el uso correcto de los sistemas de tecnología e información de sus empleados.

C. Referirá a la Oficina de Recursos Humanos para el inicio de la acción administrativa correspondiente en aquellos casos en donde se haya cometido una infracción a este reglamento.

3. Usuarios:

1. Responsable ante la Oficina de Tecnología e Información de la Guardia Nacional de Puerto Rico de:

a. Reconocen la autoridad de OTI de monitorear y controlar los servicios que están disponibles para la agencia y sus usuarios.

b. Reconocen que los sistemas de información de las entidades gubernamentales, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Gobierno de Puerto Rico y la Agencia.

c. Reconocen que los sistemas de información y las herramientas asociadas, como el correo electrónico y el Internet sólo podrán ser utilizados por aquel personal debidamente autorizado, y el uso de tales recursos constituye un *privilegio* otorgado con el propósito de agilizar los trabajos de la entidad gubernamental. Por lo tanto, los usuarios reconocen expresamente que dicho acceso a los sistemas de información no es un derecho.

d. Reconocen que la OTI no es responsable del contenido, ni por la gama de información disponible en el Internet a través de los servicios y no edita o manipula la información de ninguna manera que no sea para alcanzar los requerimientos técnicos y operacionales.

2. Seguridad de Cuentas y Contraseñas

- a. Cada usuario es responsable de tomar las medidas razonables para evitar y prevenir que su cuenta y contraseña sea conocida por alguna otra persona.
- b. Cada usuario es quien único está autorizado a utilizar su cuenta y contraseña.
- c. La contraseña será establecida por cada usuario. Será requisito que la contraseña contenga un mínimo de ocho (8) caracteres numéricos y alfa-numéricos que será cambiada cada tres (3) meses.
- d. Las cuentas y contraseñas para acceder a programas externos establecidos por otras agencias se registrarán por los parámetros establecidos por cada agencia y serán para el uso exclusivo del usuario autorizado.
- e. Las cuentas y contraseñas para aplicaciones o servicios específicos (Por ejemplo; uso de fotocopiadoras) dentro de la Agencia son para el uso exclusivo del usuario autorizado.

3. Uso del Sistema de Información y Acuerdo de Usuario

- a. Cada usuario tiene el deber de hacer todos los esfuerzos y medidas razonables para que el uso de los servicios y/o uso del Internet se haga de una manera eficiente y económica.
- b. Cada usuario tiene el deber y obligación de acatar las instrucciones, verbales o escritas, impartidas por el personal de la OTI relacionada al uso de sistemas de información y el Internet.
- c. En la eventualidad que un usuario haya obtenido o enviado inadvertidamente información sin contar con autorización para ello, debe informarlo inmediatamente a la OTI o a la gerencia una vez advenga en conocimiento de dicha situación.

- d. Todo usuario debe firmar el Acuerdo de Usuario antes que se le autorice acceso a los servicios y al Internet.

VII. Normas aplicables al Uso del Internet.

1. Los Sistemas de comunicación y acceso a la Internet son propiedad de la Guardia Nacional de Puerto Rico y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las Normas de Conducta de la Agencia y nunca con fines no oficiales o para actividades personales o con fines de lucro.
2. Las operaciones realizadas a través del Internet pueden generar responsabilidad por parte de las entidades gubernamentales del Gobierno de Puerto Rico, por lo que los usuarios que tengan acceso al Internet a través de la Agencia no tienen expectativa de privacidad alguna con relación al uso y accesos realizados a través de la Internet.
3. La Agencia se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso al Internet y el contenido de lo accedido.
4. La Guardia Nacional, a través de OTI, no se responsabiliza de la validez, calidad, contenido o corrección de la información contenida en el Internet.
5. La publicación de información de la Guardia Nacional a través de la Internet será debidamente autorizada por el Ayudante General o su representante autorizado.
6. Los usuarios que tengan autorización a utilizar computadoras tendrán acceso básico de Internet para acceder a las páginas de agencias y corporaciones públicas del Gobierno de Puerto Rico. Sólo tendrán acceso a otras páginas de Internet aquellos usuarios para los cuales sus supervisores han solicitado y justificado por escrito la necesidad de tener acceso al resto del contenido de Internet de acuerdo a las labores que realiza el usuario.
7. Tendrán acceso al Internet sin limitación los usuarios que realicen las siguientes funciones:

- A. Oficial Ejecutivo para Asuntos Estatales
- B. Ayudantes Especiales
- C. Directores de Oficinas
- D. Agentes Compradores
- E. Oficial de Contratos

8. Todo usuario que tenga acceso al Internet sin restricciones velará por hacer uso adecuado de este privilegio.

9. Queda expresamente prohibido acceder a páginas de Internet de contenido obsceno o inmoral. Todo usuario que viole esta disposición estará sujeto a las sanciones y medidas disciplinarias establecidas de acuerdo a las normas de conducta de la Agencia.

VIII. Normas aplicables al Uso de Correo Electrónico.

1. El sistema de Correo Electrónico es propiedad de la Agencia y es parte integral de sus sistemas de información, por lo que la misma se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo.

2. El correo electrónico se podrá utilizar únicamente y exclusivamente para propósitos oficiales relativos a las funciones de la Agencia.

3. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados.

4. El personal que utilicen el sistema de correo electrónico deberá velar por el cumplimiento de las normas aplicables al comportamiento de los usuarios autorizado por la entidad al momento del uso de este sistema.

IX. El Servicio de los Sistemas de Información.

1. *Códigos de Acceso y Auditoria de los Sistemas*

A. La asignación de códigos de acceso no impedirá que el uso de los sistemas de información sea auditado por el personal autorizado por la Agencia a tales fines, con el propósito de garantizar el uso apropiado de los recursos de la entidad gubernamental.

2. *Expectativa de Intimidad*

A. Los usuarios, **no tienen** expectativa de intimidad alguna con relación a la información almacenada en su computadora o que sea emitida o comunicada a través de los sistemas de información del Estado Libre Asociado de Puerto Rico.

3. *Información con Carácter de Documentos Públicos*

A. Los documentos generados o contenidos en los sistemas de información de la Agencia son parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

B. La información desarrollada, transmitida o almacenada en los sistemas de información es propiedad de la Agencia y del Estado Libre Asociado de Puerto Rico, por lo que le aplican todas las disposiciones legales relacionadas a los documentos públicos.

X. Uso de Laptops

Las Laptops son una herramienta útil y movable que la agencia puede utilizar para el funcionamiento y operación diaria de los programas de la agencia. Al igual, son un punto de riesgo a pérdida de información y equipo por accidentes, robos o cualquier otra situación inesperada. Ante esto, es necesario establecer controles que permitan minimizar los riesgos asociados al uso de éste equipo sin limitar el uso en beneficio de las operaciones de la Agencia.

A. Sólo se proveerá laptop para su uso constante en las facilidades oficiales y fuera de la Agencia a:

1. Directores de Sección o Programa.
 2. Personal que cuyas labores le requiere estar en constante movimiento y amerite comunicación digital o programas de trabajo según sea debidamente justificado por escrito por el supervisor o director del programa.
- B. El personal que sea custodio de una laptop para su uso constante será responsable de velar por el buen uso del mismo y la seguridad del equipo.
- C. En caso de pérdida por robo o accidente, deberá notificar al personal de OTI y al Encargado de la Propiedad en un periodo no mayor de veinticuatro (24) horas y hacer la querrela correspondiente con la Policía de Puerto Rico.
1. Toda pérdida de equipo se trabajará de acuerdo a los procesos de la Propiedad Estatal según establecidos por el Departamento de Hacienda y la Oficina del Contralor de Puerto Rico.
- D. La OTI proveerá laptop a los programas que así lo soliciten y justifiquen por escrito y tengan la autorización del Oficial Ejecutivo para Asuntos Estatales para funciones o actividades específicas que requieran ocasionalmente mover los sistemas de información y comunicación a otros puntos fuera de las oficinas oficiales.
- E. La OTI tendrá disponible laptops para atender cualquier situación de emergencia u operacional que requiera la reubicación de oficinas o personal y el restablecimiento de la red.
- F. La OTI proveerá los medios de comunicación y la seguridad necesaria para aquellos usuarios que ameriten llevar las laptop fuera de las oficinas oficiales y requieran acceso a la red interna de la Agencia a través de VPN y/o discado (Dial-up).

XI. Resguardos de la Información (Backups)

- A. La OTI realizará el resguardo diario de la información contenida en todos los servidores de la agencia.

- B. Los resguardos se realizarán en dos (2) ciclos diferenciales de siete (7) días.
 - 1. El primer día del ciclo consistirá de un resguardo total de la información de cada servidor. Los días subsiguientes se realizará un resguardo diferencial (Differential Backup)

- C. Los medios de resguardos serán almacenados en un lugar seguro y bajo llave fuera de las instalaciones donde se encuentran los servidores.

- D. Los usuarios serán responsables de realizar los resguardos correspondientes de toda información que se encuentre archivada en la estación de trabajo o laptop que tengan asignada para realizar sus funciones oficiales.

XII. Uso No Autorizado.

Los Usuarios de los Sistemas de Información no están permitidos a incidir en la siguiente conducta:

- A. Divulgar o compartir la contraseña (Password).

- B. Copiar, divulgar, transferir, examinar, cambiar o borrar información que está bajo la custodia de otro usuario sin la expresa autorización de éste o de la OTI.

- C. Copiar, divulgar, transferir, examinar, cambiar o borrar información o programas que le pertenecen al Gobierno de Puerto Rico y/o la Agencia sin la expresa autorización de la gerencia o de la OTI.

- D. Interferir con las operaciones del Servicio.

- E. Interferir con el servicio de Internet del Gobierno de Puerto Rico y/o de la Agencia.
- F. Evadir cualquier restricción y/o seguridad impuesta para el uso de los servicios y el Internet.
- G. Utilizar los sistemas de información para crear, guardar, transmitir o recibir mensajes o documentos de cualquier material obsceno, vulgar, ofensivo, difamatorio, repetitivo, discriminatorio por razón de género, credo, ideas políticas, origen social o nacional, que sea catalogado como de hostigamiento o de naturaleza ilegal.
- H. Utilización de protectores de pantalla (Screen Savers) con fotos, imágenes o mensajes cuyo contenido pueda resultar ofensivo o incida en conducta prohibida en el inciso 7.
- I. Uso de los sistemas de información o el Internet para obtener acceso no autorizado a cualquier otra facilidad de computadoras o servicio de sistemas de información.
- J. Copiar cualquier otro programa, data o información sin la previa autorización del dueño de los derechos de autor o de la Agencia.
- K. Enviar cualquier material por el Internet que identifique al usuario y proyecte la Agencia de manera que afecte la imagen y el nombre de esta.
- L. Utilizar los servicios y/o el Internet para crear falsas representaciones, proveer datos ficticios o anónimos.
- M. Intentar descubrir las cuentas y/o contraseñas de otros usuarios, o para esos servicios que el acceso apropiado no haya sido autorizado para ese usuario.
- N. Ejecutar cualquier acción mediante la utilización del Internet que constituya conducta inaceptable.

- O. Iniciar o continuar correos electrónicos en cadena.
- P. Utilizar el correo electrónico para beneficio personal.
- Q. Utilizar durante horas laborables cuentas de correo electrónico distintas a las provistas por la Agencia, sin el debido consentimiento de la OTI.
- R. Evitar enviar o recibir correos electrónicos y sus anejos cuya capacidad de memoria excede los diez Mega Bytes (10MB).
- S. Enviar o recibir correos electrónicos personales a su cuenta de correos electrónicos provista por la Agencia.
- T. Enviar o recibir correos electrónicos sin que el contenido y sus recipientes estén autorizados por la agencia a recibir o enviar correos electrónicos dentro del sistema de servicios de información.
- U. Acceder y abrir correos electrónicos y/o archivos solicitados provenientes del Internet cuando el antivirus notifica la posibilidad de virus.
- V. Instalar programas en cualquier equipo de los sistemas de Información para los cuales no exista una licencia o autorización válida a nombre de la Agencia.

XIII. Solicitud de servicios técnicos

- A. La OTI llevará un registro de las solicitudes, asignará un número de solicitud y asignará nivel de prioridad de acuerdo a la siguiente escala:
 - 1. Desperfectos que impidan el funcionamiento de la computadora o el periferal e imposibilite al usuario o la sección realizar su trabajo.

2. Desperfectos que afectan a la computadora o el periferal y dificultan la labor del empleado o a la sección.
 3. Malfuncionamiento que limita ciertas funcionalidades de la computadora o el periferal pero que no impiden la labor del usuario o el periferal.
- B. La OTI atenderá las situaciones referidas según el orden secuencial del registro de solicitudes pero atendiendo cada situación según el nivel de prioridad.
 - C. Las situaciones o problemas a nivel de servidor, redes (Network) y bases de datos tendrán prioridad sobre las solicitudes de servicio de los usuarios.
 - D. El registro contendrá la información básica de cada caso incluyendo la fecha de la solicitud y la fecha en que se cerró el caso.
 - E. Las solicitudes de servicio se realizarán de la siguiente manera según el caso:
 1. Desperfectos en la computadora
 - A. De existir un problema o malfuncionamiento de la computadora o uno de sus periferales, el usuario a través de correo electrónico notificará a la OTI de la situación especificando el equipo en cuestión, ubicación y una descripción detallada del problema.
 - B. En el caso que el desperfecto de la computadora impida el envío de la solicitud a la OTI, el usuario realizará la notificación por conducto de su supervisor inmediato.
 2. Malfuncionamiento de aplicaciones
 - A. De existir un problema o malfuncionamiento de una de las aplicaciones, el usuario a través de correo electrónico notificará a la OTI de la situación especificando la aplicación, una descripción detallada del problema y cómo esto afecta su trabajo.
 - B. En el caso de malfuncionamiento de aplicaciones de otras agencias, el usuario solicitará a la OTI apoyo técnico para

resolver el problema. Si el personal de la OTI entiende que es necesario solicitar apoyo técnico de la agencia externa creadora de la aplicación, dicho personal realizará la solicitud a la respectiva agencia y estará presente durante todo el proceso del servicio para brindar cualquier apoyo necesario y corroborar que el problema sea resuelto en su totalidad.

3. Problemas en la Red (Network) o el Internet

- A. De existir un problema o malfuncionamiento de la red o el Internet, notificará mediante llamada telefónica a la OTI de la situación especificando detalladamente el problema y cómo esto afecta su trabajo.
- B. El personal de la OTI registrará la llamada en el registro de solicitudes y atenderá el problema de acuerdo a los niveles de prioridad establecidos en el inciso A de este artículo.

4. Problemas en la red de Telefonía

- A. De existir un problema o malfuncionamiento de una de las líneas, extensiones, cuadro o aparato telefónico, el usuario a través de correo electrónico notificará a la OTI, con copia al oficial de utilidades de la Sección de Servicios Generales, de la situación especificando el número de extensión o línea, una descripción detallada del problema y cómo esto afecta su trabajo.
- B. El personal de la OTI registrará la situación en el registro de solicitudes y referirá y dará seguimiento del problema al DCSIM hasta que sea debidamente corregido.

XII. Infracciones

Infracciones a este Reglamento darán base para iniciar un proceso administrativo de conformidad con el Manual de Normas de Conducta y Medidas Disciplinarias de la Agencia. En casos donde el infractor sea un Contratista, podría resultar en la revocación inmediata del contrato.

XIII. Cláusula de Separabilidad

Si cualquier cláusula o disposición de este Reglamento fuere declarada ilegal o inconstitucional por un Tribunal de Justicia con jurisdicción y competencia, por sentencia final y firme, tal declaración no afectará la validez de las demás cláusulas, las

que mantendrán su validez y efecto y la declaración de nulidad o invalidez quedará limitada al artículo, sección o inciso objeto de la misma.

XII. Vigencia

Este Reglamento comenzará a regir inmediatamente a partir de la firma del mismo.

Hoy, 27 de Enero de 2011. San Juan, Puerto Rico.



ANTONIO J. VICENS

GENERAL DE DIVISION (PR)

AYUDANTE GENERAL

GUARDIA NACIONAL DE PUERTO RICO
DIVISIÓN DE SERVICIOS ADMINISTRATIVOS
OFICINA DE INFORMÁTICA

NORMAS SOBRE EL USO DE
LOS SISTEMAS ELETRÓNICOS

Normas Sobre el Uso de los Sistemas Electrónicos

La Guardia Nacional de Puerto Rico (GNPR) cuenta con acceso a computadoras, redes, servicios electrónicos internos y a la red Internet. De la única forma en que usted puede utilizar esta computadora y los servicios asociados es entendiendo y aceptando las siguientes condiciones.

Titularidad y Derechos

- *La computadora del usuario, los servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (e-mail), la Intranet, el acceso a la Internet y los documentos y programas que existen en la misma, son propiedad de la GNPR y sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o alcance del usuario.*
- *Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, por creación o modificación mediante el uso de una de las computadoras de la GNPR, será propiedad de la Agencia, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.*
- *La información contenida en esta computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mails), información de la Intranet o la Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la GNPR.*
- *Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización de uso válida a nombre de la GNPR.*
- *Se prohíbe terminantemente copiar programas de GNPR para instalarlos en otras computadoras, sin la autorización por escrito del Oficial Principal de Informática de la Agencia.*
- *Se prohíbe terminantemente el instalar programas en las computadoras de la GNPR sin la autorización por escrito del Oficial Principal de Informática de la Agencia*

- *Se prohíbe el uso de los sistemas de computadoras y comunicaciones de la GNPR para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la GNPR para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones del usuario.*
- *Se prohíbe acceder a, o utilizar propiedad intelectual (“copyrighted information”) que viole los derechos de autor.*

Seguridad

El uso de un código de acceso (“password”), no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra. Las contraseñas deben mantenerse en estricta confidencialidad y administrarse conforme al Memorando sobre medidas de seguridad adoptadas por la GNPR. Al aceptar utilizar esta computadora usted reconoce haber leído y entendido dicho Memorando.

La GNPR se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la GNPR no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de “e-mail”.

Para evitar poner en peligro la confidencialidad de la información de la GNPR, se prohíbe el envío fuera de la misma de documentos electrónicos o mensajes por medio del “e-mail” que contengan información privilegiada o confidencial.

Se prohíbe el envío o recibo de mensajes de correo electrónico entre el personal de la GNPR y otras personas que no pertenezcan a la Organización, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, religión, personas o cualquier otra situación o asunto interno de la GNPR, que puedan poner en entredicho la reputación o imagen de la Agencia, aunque la información divulgada no sea de naturaleza confidencial.

Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

Se prohíbe terminantemente codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la GNPR con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivos. En el caso de que por razones de seguridad, el Oficial Principal de Informática, permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la GNPR estará facultada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo.

Se prohíbe la modificación de los parámetros o configuración de las computadoras de la GNPR para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la Agencia.

Se prohíbe el uso de discos magnéticos o cualquier otro medio de almacenaje de información, sin que haya sido verificado o certificado como libre de virus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.

Todos los archivos que se creen en las computadoras deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo (backup) existentes.

Políticas Anti-discrimen

Se establece una prohibición absoluta y de cero tolerancia a la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica de la GNPR. Esto incluye, a modo de ejemplo, acceso a materiales eróticos,

bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discriminación de GNPR o su política de hostigamiento sexual.

Se prohíbe que se utilicen protectores de monitores (screen savers) con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que pueda resultar poco seria u ofensiva.

Se prohíbe la divulgación por cualquier medio de cualquier tipo de opiniones personales específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.

Correo Electrónico

Se prohíbe que los usuarios utilicen, durante horas laborables, cuentas de correo electrónico distintas a las cuentas oficiales provistas por la GNPR.

Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original.

Se prohíbe leer, revisar o interceptar cualquier tipo de comunicación electrónica de la GNPR o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.

Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias (newsgroups) que divulguen información o mensajes ajenos a las funciones y deberes del usuario.

No se podrá crear archivos o enviarlos mediante el correo electrónico que exceda la capacidad de la cuota del usuario en el servidor.

Disposiciones Misceláneas

Se prohíbe el uso de programas de charlas (Chats) a menos que sean autorizados expresamente por el Oficial Principal de Informática de la GNPR. El usuario deberá establecer que el uso de este programa está directamente relacionado con las funciones establecidas.

Las políticas antes mencionadas sobre el uso del correo electrónico y sus auditorías serán de igual aplicación para los otros recursos de la Intranet e Internet tales como el WWW, FTP, Chat, etc.

Es responsabilidad de los usuarios el cumplir con las normas de cuotas de espacio en los servidores.

Las políticas de Internet serán revisadas periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la GNPR. Se incorporan y se hacen formar parte de estas advertencias todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que sean pertinentes al uso de las computadoras en la Agencia.

Procedimientos Disciplinarios

Se tomarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso a la Internet, según sea el caso. En el caso de aplicación de medidas disciplinarias las mismas se regirán conforme al Manual de Normas y Conductas de la GNPR.

La GNPR se reserva el derecho de radicar acusaciones criminales por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.

Entiendo las normas citadas y acepto que se ha divulgado toda la información relacionada al uso de esta computadora. Además, el personal cualificado de GNPR está disponible para aclarar las dudas que me surjan en cuanto al cumplimiento de estas condiciones de uso.

Aceptación

Acepto que es mi obligación conocer y seguir todas las políticas e instrucciones de la GNPR en cuanto a las medidas de seguridad del uso del equipo de computadoras y de las redes disponibles, particularmente las Normas adoptadas para la utilización del Internet.

El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos de la GNPR no esté contemplada en estas

advertencias y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio del encargado se trata de una conducta o actuación impropia o irresponsable en relación a los referidos equipos y recursos electrónicos. A los fines de estas advertencias y condiciones de uso, una conducta o actuación impropia o irresponsable significa cualquier acción directa o indirecta que ponga en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas de la GNPR. Uso impropio o irresponsable significa además, cualquier actuación o conducta directa o indirecta que pueda ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios, o personas ajenas a la GNPR.

Acepto además, que es mi obligación comunicar al Oficial Principal de Informática de la GNPR, cualquier situación, incidente o problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas, que surja en el uso de las computadoras o redes de la GNPR.

Estas Normas comenzarán a regir inmediatamente a partir de la firma de las mismas.

Hoy, 27 de Enero de 2011, San Juan, Puerto Rico.



ANTONIO J. VICENS

GENERAL DE DIVISION (PR)

AYUDANTE GENERAL

**GUARDIA NACIONAL DE PUERTO RICO
DIVISIÓN DE SERVICIOS ADMINISTRATIVOS
OFICINA DE INFORMÁTICA**

PLAN DE CONTINUIDAD OPERACIONAL

GUARDIA NACIONAL DE PUERTO RICO
OFICINA DE INFORMATICA
PLAN DE CONTINUIDAD OPERACIONAL

Tabla de Contenido

A. Propósito.....	1
B. Localización de la Oficina de Informática.....	1
C. Medidas de Control a Tomarse en consideración en la Oficina de Informática en caso de que ocurra una emergencia y/o desastre.....	1
D. Responsabilidades del Personal de la Oficina.....	1-2
E. Responsabilidades del Grupo Técnico de la Oficina de Informática.....	2
F. Medidas de Control y Seguridad en Casos de Emergencia.....	2-3
G. Medidas de Recuperación Después de un Caso de Emergencia.....	4
H. Guías para Resguardo.....	4
I. Grupos de Recuperación.....	4
J. Itinerario de Restauración.....	4-5
K. Aplicaciones.....	5
L. Configuración de Programas.....	5
M. Inventario de Equipo.....	5-6
N. Dependencias Estatales en Caso de Emergencia y/o Desastres.....	6

GUARDIA NACIONAL DE PUERTO RICO

OFICINA DE INFORMÁTICA

A. PROPÓSITO

Los procedimientos descritos en este plan han sido diseñados con el propósito de establecer las medidas de seguridad necesarias para proteger el personal, equipo y propiedad de la Oficina de Informática en caso de incendios, desastres naturales como terremotos, huracanes, y desastres provocados por actos de terrorismo.

Este plan permitirá establecer y mantener en funcionamiento la Oficina de Informática de manera que oriente y capacite al personal para enfrentarse a situaciones de emergencia. Además, especificará los deberes y responsabilidades de cada empleado de manera que puedan tomar medidas preventivas para la conservación y seguridad de la planta física, propiedad, equipo, etc., así como hacer las asignaciones correspondientes durante la emergencia.

B. LOCALIZACIÓN DE LA OFICINA DE INFORMÁTICA

La Oficina de Informática de la Guardia Nacional de Puerto Rico está localizada en la Calle General Esteves, Parada 3 1/2, Puerta de Tierra, San Juan, PR 00902. División de Servicios Administrativos, Teléfono (787)721-3131 (Ext.7038, 7039,7001.

C. MEDIDAS DE CONTROL A TOMARSE EN CONSIDERACION EN LA OFICINA DE INFORMÁTICA EN CASO DE QUE OCURRA UNA EMERGENCIA Y/O DESASTRE:

La Oficina de Informática de GNPR ha establecido un plan de resguardo el cual tiene como propósito identificar los pasos y medidas necesarias para salvaguardar los activos y garantizar el restablecimiento de las operaciones de la oficina.

En este plan se establecen las responsabilidades de la Oficina de Informática para la obtención y almacenamiento de la información, además, incluye la frecuencia del proceso e itinerarios de resguardos.

Su objetivo es proveer una guía para mantener la integridad del sistema de información de la GNPR, además de asegurar el restablecimiento de los procesos en aquellos casos donde la base de datos principal o las facilidades donde se ubica la misma queden inoperantes. Su alcance es identificar archivos corrientes que se deben salvaguardar y su frecuencia de resguardo. Establece también las responsabilidades por función, documentación actualizada y mantenimiento necesario para darle continuidad y mantener el plan efectivo a través del tiempo; independientemente de cambios y/o crecimiento de la oficina.

D. RESPONSABILIDADES DEL PERSONAL DE LA OFICINA PARA LA PROTECCIÓN Y SEGURIDAD DEL EQUIPO DE INFORMÁTICA

1. El empleado que se encuentre en su área de trabajo deberá velar lo siguiente:

- Cerrar todos los archivos en los cuales está trabajando; remover y guardar los discos.
- Apagar todos los sistemas a su cargo.
- Apagar la impresora o cualquier otro equipo en el área.
- Desconectar todos los equipos de las tomas eléctricas.
- Cubrir los equipos con bolsas plásticas para protegerlos de humedad.
- Retirar cualquier equipo que esté cerca de una ventana.

2. Al finalizar la emergencia, realizar inventario tanto del equipo como del área de trabajo y verificar la toma eléctrica que esté en buenas condiciones; de lo contrario, deberá informar el desperfecto a su supervisor inmediato y este a la División de Ingeniería. Luego deberá asegurarse de que:
 - Ninguna de las bolsas plásticas de los equipos estén húmedas.
 - El monitor no tenga rota la pantalla.
 - La impresora esté en buenas condiciones.
 - De encontrar algún equipo roto, no intente operarlo.
3. De existir algún problema en lo antes expuesto, prepare un informe de daños el cual debe contar con lo siguiente:
 - Su nombre, fecha, hora.
 - Sección para la cual trabaja, número de estación y número de extensión.
 - Descripción del equipo que considera dañado.
 - Detalle en forma breve lo que se entendió le pasó al equipo.
4. Terminado el informe entregarlo al administrador de la red.

E. RESPONSABILIDADES DEL GRUPO TÉCNICO DE LA OFICINA DE INFORMÁTICA

El personal técnico de la Oficina de Informática será responsable de:

1. Mantenerse en constante comunicación y monitoreo de la oficina (antes, durante y después de la emergencia).
2. Estar a disposición el tiempo necesario en que se necesiten sus servicios.
3. Tomar las medidas de seguridad y precauciones necesarias para que no se afecten los servicios esenciales.
4. Mantener informado en todo momento al Oficial Ejecutivo.

F. MEDIDAS DE CONTROL Y DE SEGURIDAD EN CASOS DE EMERGENCIA

1. AVISO DE EXPLOSIVOS

- La persona que reciba la llamada deberá anotar la hora exacta en que se recibió la misma.
- Notificar inmediatamente al supervisor inmediato y al Oficial Ejecutivo para Asuntos Estatales.
- Cuando se notifica al personal que está bajo una alarma de explosivos, el mismo deberá de permanecer en su área hasta tanto se reciban órdenes de abandonar la oficina.
- Es importante familiarizar al personal con los medios de salida del edificio y/u oficina y como usarlos de manera segura y eficiente. El orden y control son los factores más importantes a observarse, a los fines, no solamente de evitar accidentes, sino evitar caer en estado de pánico y como consecuencia, la pérdida de vidas.
- No se permitirá el movimiento de personas en dirección contraria.
- Las puertas con libre acceso estarán rotuladas con la frase "EXIT" o "SALIDA".
- Todo el personal obedecerá las órdenes emitidas por las personas autorizadas y seguirán las rutas de desalojo establecidas.

2. MEDIDAS DE DESALOJO EN CASO DE INCENDIO

- Todo el personal deberá adiestrarse en la manera de cómo utilizar los extintores.
- Cada empleado deberá conocer la localización de los extintores.
- Los extintores se colocarán en lugares visibles y accesibles.
- La primera persona que detecte un incendio deberá dar alerta inmediatamente, y deberá, en la medida que sea posible, intentar apagar el fuego haciendo uso de los extintores y tomando las debidas precauciones. De no lograr apagarlo deberá comunicarse vía telefónica con el Cuerpo de Bomberos.

3. MEDIDAS DE SEGURIDAD EN CASO DE UN FENÓMENO ATMOSFÉRICO

- Planificar el tiempo debidamente y realizar los preparativos para evitar los inconvenientes antes de que llegue el fenómeno atmosférico.
- Si ocurre durante fin de semana o día feriado, estar atento para determinar el día que se asistirá a la oficina para dejar en un lugar seguro los objetos sueltos que haya dentro de la oficina tales como: máquinas, tiestos, escritorios, zafacones, etc.
- Siempre se debe mantener la calma, no prestar atención a rumores.
- No hacer llamadas telefónicas innecesarias.
- Almacenar en un lugar seguro los objetos sueltos que haya dentro de la oficina tales como: máquinas, tiestos, escritorios, zafacones, etc.
- Tomar precauciones con el uso de linternas, lámparas o velas, para evitar incendios.
- La succión creada por la diferencia en la presión atmosférica dentro y fuera de la oficina puede destruir ventanas o puertas. Para evitar esto abra una ventana o puerta en el lado opuesto a la dirección que normalmente sopla el viento.
- Pasado el fenómeno atmosférico, no toque ninguna línea eléctrica. Informe, si es posible, a la Autoridad de Energía Eléctrica, Defensa Civil o el Cuerpo de Bomberos.

4. MOVIMIENTOS TELÚRICOS (SISMOS/TERREMOTOS)

- Si el terremoto o sismo ocurre estando usted dentro de la oficina, manténgase adentro. Proteja su vida bajo un escritorio, una mesa, bajo el marco de una puerta, en los pasillos o contra las paredes interiores. Manténgase lejos de cristales y puertas que dan al exterior.
- No utilice velas, fósforos u otros objetos inflamables ya sea durante o después del sismo. Apague, en la medida que sea posible y si tiene las facilidades y/o equipo, cualquier incendio que se haya originado.
- Si el terremoto ocurre estando fuera del edificio donde está ubicada la oficina, evite el contacto con cables eléctricos hasta que el sismo termine.
- No corra cerca o entre a edificios, uno de los mayores peligros radica en la caída de pedazos de vidrio o bloques de niveles altos.
- Si se encuentra en un vehículo de motor cuando sucede el sismo, detenga el mismo tan pronto la sea posible de manera que no ocasione accidentes.

G. MEDIDAS DE RECUPERACIÓN DESPUÉS DE UNA EMERGENCIA

1. Verifique si hay lesionados. No trate de mover personas seriamente lesionadas a no ser que éstas se encuentran en peligro de perder la vida.
2. Coteje las instalaciones de agua y luz para verificar si hay averías, pero no las ponga a funcionar. En caso de un terremoto, el movimiento telúrico puede haber agrietado los conductos eléctricos y de agua.
3. No use el teléfono, a no ser que sea una emergencia, esta medida puede salvar muchas vidas.
4. No se vaya de paseo a observar los daños, es necesario mantener las áreas despejadas.
5. Manténgase fuera de edificios que hayan sido seriamente afectados.
6. En caso de terremoto prepárese para hacerle frente a sacudidas adicionales.

H. GUIAS PARA RESGUARDO (BACK-UPS)

1. Obtener cinta magnética de resguardo para la ejecución del proceso.
2. Realizar un resguardo completo de lunes a viernes al concluir los trabajos de producción.
3. Identificar y anotar cualquier anomalía o problema en la ejecución de los procesos (hardware & software).
4. Los resguardos se distinguirán con unas etiquetas externas "LABELS" para identificar el contenido de la información.

I. GRUPOS DE RECUPERACIÓN

<u>GRUPO</u>	<u>COMPONENTES</u>	<u>FUNCIÓN</u>	<u>PERSONAL</u>
A	Gerencia	Decisiones Gerenciales	Director(a) Ejecutivo(a)
B	Finanzas/Informática	Coordinación – Reportar Grupo A	Director(a) de Finanzas y Director(a) de Informática
C	Informática	Restauración y Operación	Director(a) de Informática

J. ITINERARIO DE RESTAURACIÓN

<u>TAREA</u>	<u>GRUPO</u>	<u>DESCRIPCIÓN</u>
1	A	Activar el Plan.
2	A	Notificar a las organizaciones de servicio y emergencia.
3	B	Notificar al grupo de restauración.
4	B	Verificar el status del personal de informática.
5	B,C	Verificar daños y estado general de los sistemas.
6	C	Analizar opciones de recuperación y confirmar la decisión de utilizar los servicios de recuperación.

7	C	Notificar y activar los servicios de recuperación.
8	B	Notificar a los diferentes suplidores de equipo y otros productos sobre la emergencia y alertarlos sobre las posibles necesidades.
9	C	Activar el Grupo de Restauración.
10	B	Activar el Grupo Operacional.
11	C	Identificar y relocalizar equipo, archivos e inventario. Relocalizar respaldos de bóvedas externas al Centro Alterno.
12	B,C	Reunirse con suplidores e identificar necesidades para la restauración.
13	A,C	iniciar restauración de utilidades generales y seguridad.
14	C	Restaurar la data, programas, y las telecomunicaciones.
15	C	Reconstruir el medio ambiente de producción.
16	A,B,C	Revisar tiempo de restauración e itinerarios.
17	C	Conducir pruebas de los sistemas y verificar operaciones del Centro Primario.
18	A,B	Notificar a todos los miembros de grupos, clientes y suplidores sobre la relocalización al Centro Primario.
19	C	Reconstruir archivos de producción y librerías.
20	C	Relocalizar el procesamiento de programas y archivos de producción al Centro Primario.
21	C	Revisar el procesamiento y buen funcionamiento de todas las aplicaciones.
22	C	Relocalizar todo el inventario y descontinuar el uso y accesos al Centro Alterno. Crear respaldos de archivos críticos de sistema y producción.
23	A,B,C	Evaluar el evento y actualizar el Plan de Continuidad de Negocio.

K. APLICACIONES

<u>APLICACIÓN</u>	<u>PERSONA RESPONSABLE</u>	<u>CLASIFICACIÓN</u>
Microsoft Exchange	Director(a) de Informática	Indirecta
PRIFAS y RHUM Kronos WFC 6.0	Director(a) de Finanzas Director de Rec. Hum. y Director(a) de Informática	Interna Externa
MIP Accounting Microix	Director(a) de Finanzas y Director(a) de Informática	Interna Externa

La tarea para restaurar estas aplicaciones es localizar el resguardo más reciente y restaurarlo en el Centro Alterno.

L. CONFIGURACIÓN DE PROGRAMAS

La configuración de los sistemas operativos utilizados en la GNPR, es Windows XP SP3 en los estaciones de trabajo y Windows Server 2003 SP1 en los servidores.

M. INVENTARIO DE EQUIPO

El propósito de esta sección es proveer un detalle de toda la configuración de los sistemas (equipo) del Centro Primario.

- **Inventario del Equipo del Centro de Datos Primario:**

<u>MARCA</u>	<u>MODELO</u>	<u>SERVIDOR</u>	<u>SISTEMA OPERATIVO</u>	<u>USO</u>
HP	Dell Power Edge 2600	GNPR Exchange_01	Windows Server 2003 SP1	Active Directory, PDC Emulator, DHCP, DNS, IIS, WINS Email Server
HP	Proliant ML350	GNPR-Firewall-isa	Windows Server 2003 SP1	ISA Firewall, Backup Server
HP	Dell Power Edge 2400	GNPR-Fil-Prt-01	Windows Server 2003 SP1	Active Directory, DNS, DHCP, WINS, File Print Server
HP	Storage Works AIO400	GNPR-san	Windows Storage Server 2003 SP1	WSUS, PRIFAS RHUM File Server, ISCSI Hosting, Doculex Web Server
HP	Dell Power Edge 2600	GNPR-Db-01	Windows Storage Server 2003 SP1	Data Base Server SQL SERVER MIP, MICROIX
HP	Proliant ML 359 G-6	GNPR-Kronos-Db	Windows Server 2003 SP2	Data Base Server SQL SERVER Kronos WFC 6.0
HP	Proliant ML 359 G-6	GNPR-Kronos-Tel	Windows Server 2003 SP2	Kronos Tele Time

El equipo necesario para cumplir con el proceso de restauración es el siguiente:

<u>SISTEMA OPERATIVO</u>	<u>PROCESSOR</u>	<u>RAM</u>	<u>HDD</u>	<u>USO</u>
Windows Server 2008	Intel Xeon E5530	4GB	500GB	Active Directory, ISA Firewall, Web Server, Backup Server, WSUS, MIP, MICROIX
Windows Server 2008 (utilizando virtualización)	2x Intel Xeon E5530	16GB	1TB	Active Directory, PDC Emulator, DHCP, DNS, Email, File, Print Server
Windows Server 2008	Intel Xeon E5530	8GB	500GB	Kronos WFC 6.0 y Tele Time, SQL

N. DEPENDENCIAS ESTATALES EN CASO DE EMERGENCIAS Y/O DESASTRES

<u>Agencia</u>	<u>Teléfono</u>
Cuerpo de Bomberos	(787) 343-2330
Cuerpo de Emergencias Médicas	(787) 775-0550
Policía de Puerto Rico	(787) 343-2020
Manejo de Emergencias (AEMEAD)	(787) 724-0124
Servicio Nacional de Meteorología	(787) 253-4586
Cruz Roja Americana	(787) 729-9400

O. VIGENCIA

Este Plan comenzará a regir a partir de la firma del mismo.

Hoy, 27 de Enero de 2011, San Juan, Puerto Rico.



ANTONIO J. VIGENS

GENERAL DE DIVISION (PR)

AYUDANTE GENERAL