

SECRETARÍA GENERAL

SG-OFICIO-14012-2019

Guatemala, 6 de septiembre de 2019

Ingeniero
Rodolfo Estuardo Arriaga Herrera
Director Ejecutivo
Registro Nacional de las Personas -RENAP-
Su Despacho.

Registro Nacional de las Personas
-RENAP-
RECEBIDO
- 6 SEP 2019
DIRECCIÓN EJECUTIVA
FIRMA:  HORA: 15:35

Estimado Ingeniero Arriaga:

Enviándole un atento y cordial saludo, me permito remitirle Informe de Auditoría Informática del 01 de Enero de 2015 al 31 de Octubre de 2016 al Registro Nacional de las Personas –RENAP-, proveniente del Subcontralor de Calidad del Gasto Público, Contraloría General de Cuentas.

Lo anterior para el diligenciamiento que su persona considere oportuno a efecto de girar las instrucciones que considere pertinente.

Sin otro particular me es grato suscribirme.

Atentamente.


Registro Nacional de las Personas -RENAP-
SECRETARÍA GENERAL
RENAP
Registro Nacional de las Personas
Lic. Marco Antonio Posadas Pichillá
Secretario General
Secretaría General
Sede Central Renap Guatemala, Guatemala

CONTRALORÍA GENERAL DE CUENTAS

**REGISTRO NACIONAL DE LAS PERSONAS -RENAP-
INFORME DE AUDITORÍA INFORMÁTICA
DEL 01 DE ENERO DE 2015 AL 31 DE OCTUBRE DE 2016**



GUATEMALA, JUNIO DE 2019



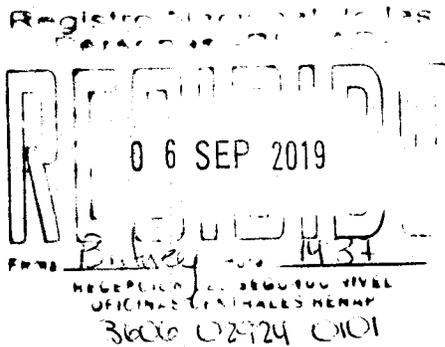
Contraloría General de Cuentas
GUATEMALA, C.A.

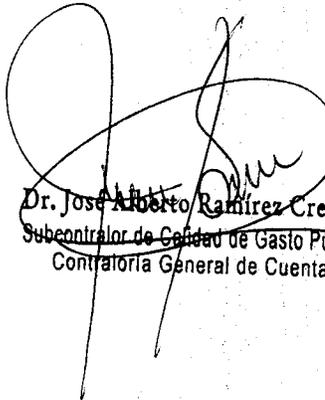
Guatemala, 05 de septiembre de 2019

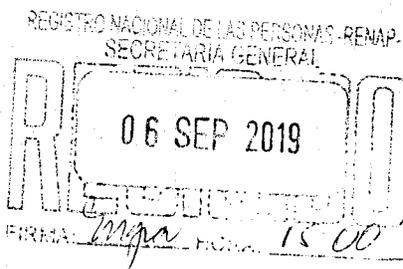
Señor (a) :

En mi calidad de Subcontralor de Calidad de Gasto Público y en cumplimiento de lo regulado en la literal k) del artículo 13 de la Ley Orgánica de la Contraloría General de Cuentas y sus reformas, conforme la delegación que oportunamente me fuera otorgada, hago de su conocimiento de manera oficial el informe de auditoría realizado por el equipo de auditores designados mediante nombramiento (s) número (s) DAS-12-0009-2017, quienes de conformidad con el artículo 29 de la precitada Ley Orgánica son responsables del contenido y efectos legales del mismo.

Sin otro particular, atentamente.




Dr. José Alberto Ramírez Crespin
Subcontralor de Calidad de Gasto Público
Contraloría General de Cuentas





CONTRALORÍA GENERAL DE CUENTAS

**REGISTRO NACIONAL DE LAS PERSONAS -RENAP-
INFORME DE AUDITORÍA INFORMÁTICA
DEL 01 DE ENERO DE 2015 AL 31 DE OCTUBRE DE 2016**



GUATEMALA, JUNIO DE 2019



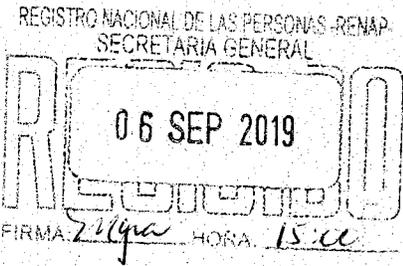
ÍNDICE	Página
1. INFORMACIÓN GENERAL	1
Base Legal	1
Función	1
2. FUNDAMENTO LEGAL DE LA AUDITORÍA	1
3. OBJETIVOS DE LA AUDITORÍA	2
Área Técnica	2
Generales	2
Específicos	2
4. ALCANCE DE LA AUDITORÍA	3
Área Técnica	3
5. COMENTARIOS Y CONCLUSIONES	3
Comentarios	3
Conclusiones	6
6. RESULTADOS DE LA AUDITORÍA	8
Hallazgos Relacionados con el Control Interno (Área Técnica)	8
7. AUTORIDADES DE LA ENTIDAD, DURANTE EL PERÍODO AUDITADO	82
8. COMISIÓN DE AUDITORÍA	83
ANEXOS	84
Nombramiento	
Formulario Estadístico	
Forma SR1	





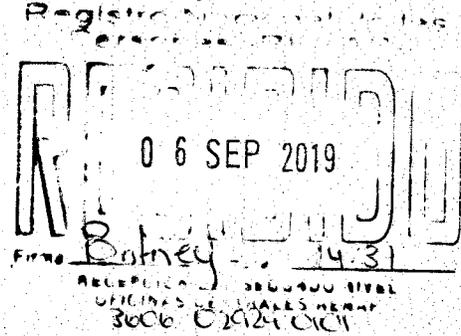


Contraloría General de Cuentas
GUATEMALA, C.A.



Guatemala, 06 de junio de 2019

Licenciado
Cesar Son Ardon
Director Ejecutivo en Funciones
Registro Nacional de las Personas -RENAP-



Señor (a) Director Ejecutivo en Funciones:
Los Auditores de la Contraloría General de Cuentas de Auditoría Informática designados de conformidad con el (los) Nombramiento (s) No. (s) DAS-12-0009-2017 de fecha 18 de mayo de 2017, hemos efectuado auditoría informática, en el (la) Registro Nacional de las Personas -RENAP-, con el objetivo de evaluar el proceso de la emisión del Documento Personal de Identificación -DPI- y las funciones de la Dirección de Informática y Estadística.

El trabajo de auditoría consistió en verificar la Planificación y Organización de TI, Infraestructura de TI y la Seguridad de la información, durante el periodo comprendido del 01 de enero de 2015 al 31 de octubre de 2016.

Hallazgos relacionados con el Control Interno

Área Técnica

1. Vulnerabilidad en la seguridad de los servicios de la red interna
2. Falta de procedimientos para el uso de bitácoras
3. Desactualización de los Parches en la base de Datos
4. Falta de un Plan de Continuidad del Negocio -BCP-
5. Falta de un oficial de seguridad
6. Falta de seguridad y condiciones apropiadas en el área de trabajo
7. Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos

La auditoría fue practicada por el (los) auditor (es) en sistemas informáticos: Ing. Erickson Alexander Aqueche Padilla, Lic. Byron Alfredo Galindo Arauz (Coordinador) y Lic. Angel Estuardo Sandoval Villatoro (Supervisor)







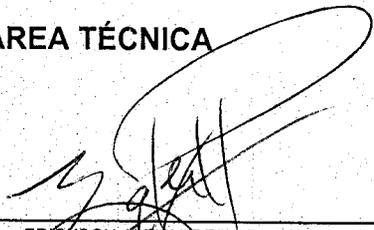
Contraloría General de Cuentas
GUATEMALA, C.A.

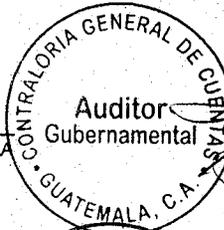
Los comentarios y conclusiones que se determinaron se encuentran en detalle en el informe de auditoría adjunto.

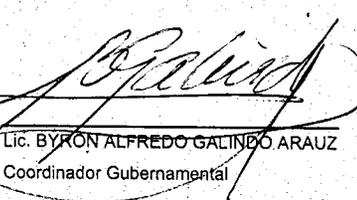
El (los) hallazgo (s) contenido (s) en el presente informe, fue (fueron) discutido (s) por la comisión de auditoría con las personas responsables.

Atentamente,

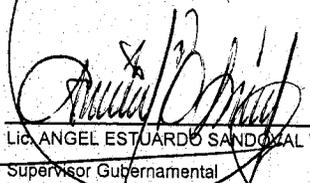
ÁREA TÉCNICA


Ing. ERICKSON ALEXANDER AQUECHE PADILLA
Auditor Gubernamental




Lic. BYRON ALFREDO GALINDO ARAUZ
Coordinador Gubernamental




Lic. ANGEL ESTUARDO SANDOVAL VILLATORO
Supervisor Gubernamental





1. INFORMACIÓN GENERAL

Base Legal

El Registro Nacional de las Personas -RENAP-, fue creado según Decreto Número 90-2005 del Congreso de la República, en el cual indica en su Artículo 1 Creación "Se crea el Registro Nacional de las Personas, en adelante RENAP, como una entidad autónoma, de derecho público, con personalidad jurídica, patrimonio propio y plena capacidad para adquirir derechos y contraer obligaciones. La sede del RENAP, está en la capital de la República, sin embargo, para el cumplimiento de sus funciones, deberá establecer oficinas en todos los municipios de la República; podrá implementar unidades móviles en cualquier lugar del territorio nacional, y en el extranjero, a través las oficinas consulares".

Función

Las funciones esenciales del Registro Nacional de las Personas -RENAP-, están reguladas en el Decreto 90-2005, Artículo 2 Objetivos "El RENAP es la entidad encargada de organizar y mantener el registro único de identificación de las personas naturales, inscribir los hechos y actos relativos a su estado civil, capacidad civil y demás datos de identificación desde su nacimiento hasta la muerte, así como la emisión del Documento Personal de Identificación. Para tal fin implementará y desarrollará estrategias, técnicas y procedimientos automatizados que permitan un manejo integrado y eficaz de la información, unificando los procedimientos de inscripción de las mismas".

2. FUNDAMENTO LEGAL DE LA AUDITORÍA

La auditoría se realizó con base en:

La Constitución Política de la República de Guatemala, según lo establecido en el artículo 232.

Ley Orgánica de la Contraloría General de Cuentas, Decreto Número 31-2002, artículos: 2. Ámbito de Competencia y 4. Atribuciones:

Reglamento de la Ley Orgánica de la Contraloría General de Cuentas, Acuerdo Gubernativo No. 9-2017, artículo 2. Ámbito de Aplicación.

Acuerdo Gubernativo Número 130-2017, Reforma al Acuerdo Gubernativo Número 9-2017.





Acuerdos A-57-2006 y 09-03 de la Contraloría General de Cuentas, que aprueban las Normas de Auditoría del Sector Gubernamental y Normas Generales de Control Interno.

Acuerdo No. A-028-2012 de la Contraloría General de Cuentas de fecha 02 de marzo 2012, rendición de informes.

Nombramiento (s) DAS-12-0009-2017 de fecha 18 de mayo de 2017.

3. OBJETIVOS DE LA AUDITORÍA

Área Técnica

Generales

Practicar Auditoría de Sistemas Informáticos al proceso de la emisión del Documento Personal de Identificación -DPI- y a las funciones de la Dirección de Informática y Estadística, verificando la Planificación y Organización, Infraestructura de TI y la Seguridad de la Información, en el Registro Nacional de las Personas -RENAP-, durante el período comprendido del 01 de enero de 2015 al 31 de octubre de 2016.

Específicos

Verificar el proceso completo de la emisión del Documento Personal de identificación -DPI- en la Dirección de Procesos del Registro Nacional de las Personas -RENAP.

Verificar en la Dirección de Informática y Estadística, las funciones asignadas a la planificación y organización de las TI, al Recurso Humano de TI, a la Infraestructura instalada en TI y la Seguridad de la Información implementada.

Verificar la seguridad e integridad del Sistema de Registro Civil -SIRECI-.

Verificar los manuales de operación, de usuario y de Mantenimiento del área de informática.



4. ALCANCE DE LA AUDITORÍA

Área Técnica

Evaluar el proceso completo de la emisión del Documento de Identificación Personal -DPI- y las funciones de la Dirección de Informática y Estadística, verificando la Planificación y Organización de TI, Infraestructura de TI y la Seguridad de la Información, por el periodo comprendido del 01 de enero de 2015 al 31 de octubre de 2016.

5. COMENTARIOS Y CONCLUSIONES

Comentarios

En la Unidad de Seguridad Informática del Registro Nacional de las Personas -RENAP-, se evaluó el comportamiento del portal web ante eventos de Denegación de Servicio, al realizar la prueba respectiva, se determinó que no es capaz de soportar este tipo de eventualidades. Así mismo se identificó que en dos formularios uno para consultar el estado del trámite del Documento de Identificación Personal -DPI- y un formulario, el cual solicita usuario y contraseña, el certificado SSL (Secure Socket Layer) que encripta el tráfico sobre el protocolo Https, era identificado por el navegador como no seguro. Al evaluar en el portal web, si era posible visualizar el código html, se determinó que con utilizar click derecho sobre algún área se puede visualizar con facilidad.

Otra evaluación que se realizó en compañía del personal técnico del Departamento de Seguridad, del Registro Nacional de las Personas -RENAP-, fue la de escanear los equipos conectados a la red interna de la institución, localizando dos impresoras, en las cuales el usuario de administrador no tenía configurada una contraseña y era posible realizar configuraciones como la de asignar una contraseña al usuario administrador y modificar la dirección IP. Así mismo se determinó que en las impresoras se encontraban habilitados varios puertos para ingresar a la consola de administración.

El servidor de correo institucional del -RENAP- está a cargo del Departamento de Seguridad Informática, se determinó en base a la prueba insitu con el encargado de seguridad, la cual consistió en configurar una cuenta de correo electrónico en un equipo que utilizaba Microsoft Outlook y se pudo constatar que las credenciales que se requerían para efectuar la entrada (logear) únicamente era el usuario de red y su contraseña, no tomando en cuenta la dirección de correo electrónico.





Se solicitó a la Dirección de Informática y Estadística, ingresar al Centro de Datos para realizar una inspección de la Granja de Servidores donde se encuentra alojada la SAN con los diferentes servidores físicos como virtualizados, así como los equipos y estanterías donde se encuentran resguardadas las cintas de los backups (Cintotecas), al efectuar la evaluación se pudo determinar que el Data Center esta en proceso de remodelación, por lo que se recomendó que el piso sea el adecuado, que la puerta para el ingreso no sea de madera, que los racks y gabinetes del cableado sean certificados, y que se instalen sensores de movimiento, de humedad y temperatura.

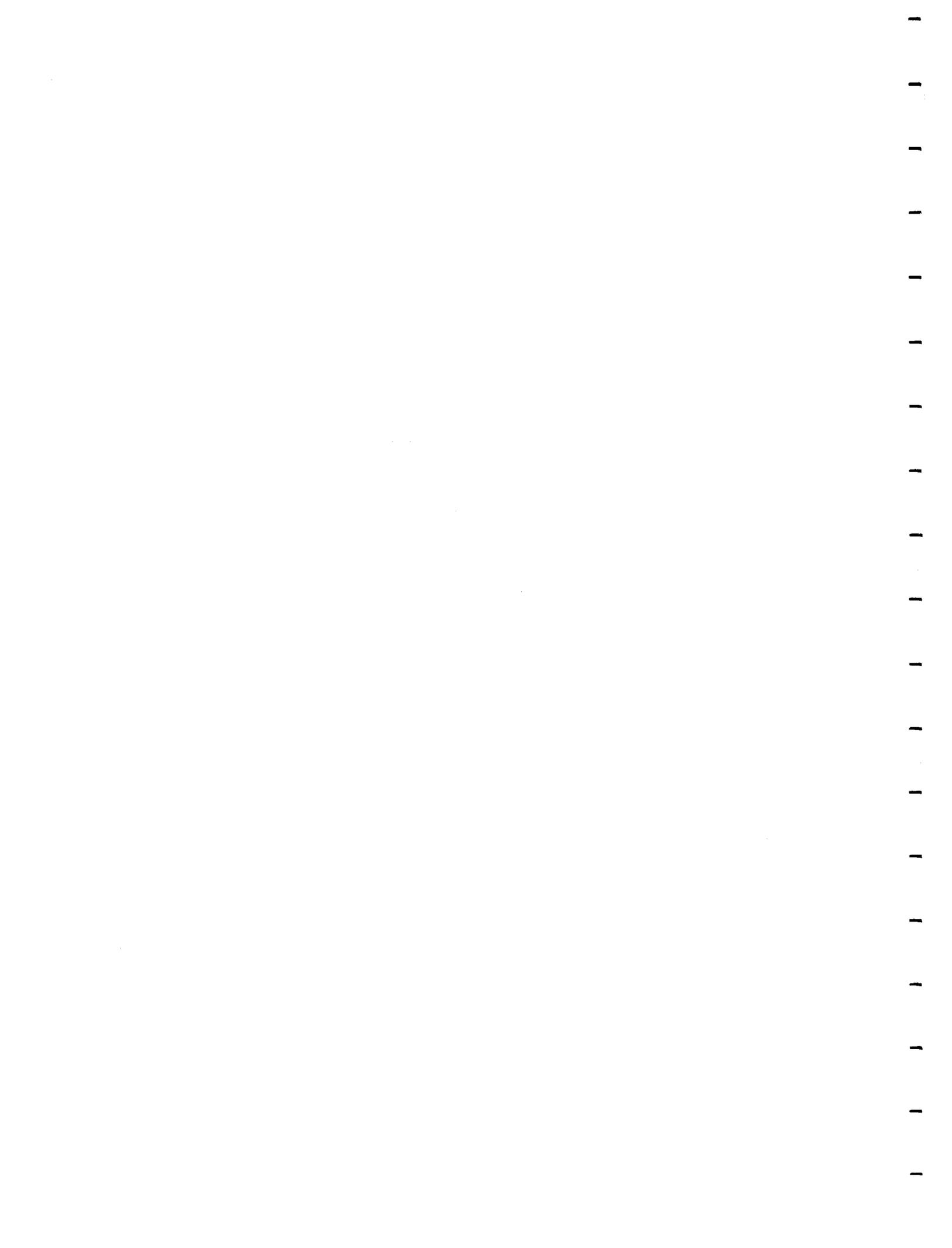
Al momento de efectuar las revisiones de los backups, se observó que se llevan en forma incremental de los diferentes servidores que aloja la base de datos del Sistema del Registro Civil -SIRECI-, determinando que son alojados en el mismo servidor de producción.

Se evaluó el Sistema del Registro Civil -SIRECI-, el cual posee una base de datos en Oracle 11G y su versión inicial fue desarrollada en Visual Basic, dicho sistema se utiliza para llevar a cabo el registro de las personas, para guardar la información relativa a los hechos y actos de las personas naturales, desde su inscripción por nacimiento hasta su defunción. Así también se evaluó el Sistema de Identificación Biométrico -SIBIO- y AFIS (Automated Fingerprint Identification System), que sirven de reconocimiento facial e identificación Biométrica y el registro de las huellas dactilares, para la emisión del Documento de Identificación Personal -DPI-. Así también se evaluó el sistema de nóminas, determinando que se lleva en hojas de excel desde hace más de 10 años y que todavía no están adheridos a Guaténominas, así mismo se verificó el sistema de control biométrico determinando que cumple su función de registrar las marcas de las entradas y salidas del personal.

Se observó que a la fecha de la auditoría, no existía un procedimiento definido que indique los pasos a seguir por parte del Administrador de la Base de Datos, en donde se consigne o se nombre a una comisión que mantenga el control, presencia y garantice que se realizó la modificación o cambio en la base de datos conforme lo solicitado por el dueño de la información y no queda plasmado en Acta Administrativa.

Se evaluó la unidad de Base de Datos de la Dirección de Informática y Estadística, al verificar el sistema gestor de la base de datos, se determinó que tiene acceso el Administrador de la Base de Datos (DBA) al AUDIT_TRAIL, que se encuentra activo, y que el Jefe de la unidad lo utiliza para llevar el control de las acciones que realizan los administradores de las bases de datos (DBA's). Además se observó que no existe un procedimiento para efectuar actualizaciones a los parches del Sistema Gestor de Base de Datos, así mismo, no cuentan con una





plataforma de hardware que sea utilizada como ambiente de pruebas para realizar un análisis antes de la implementación de los parches en la Base de Datos de producción.

Al realizar la evaluación en el Departamento de Soporte Técnico, se determinó que el personal técnico es el encargado de realizar las configuraciones en los equipos de cómputo de la institución, utilizando un usuario genérico de administración local, los cuales están controlados. Así mismo se observó que ninguna persona que pertenezca al Departamento de Soporte Técnico, participa en la realización de backup y borrado de la información que contiene los equipos de cómputo, solo si es a petición de los usuarios responsables de la información y del equipo asignado.

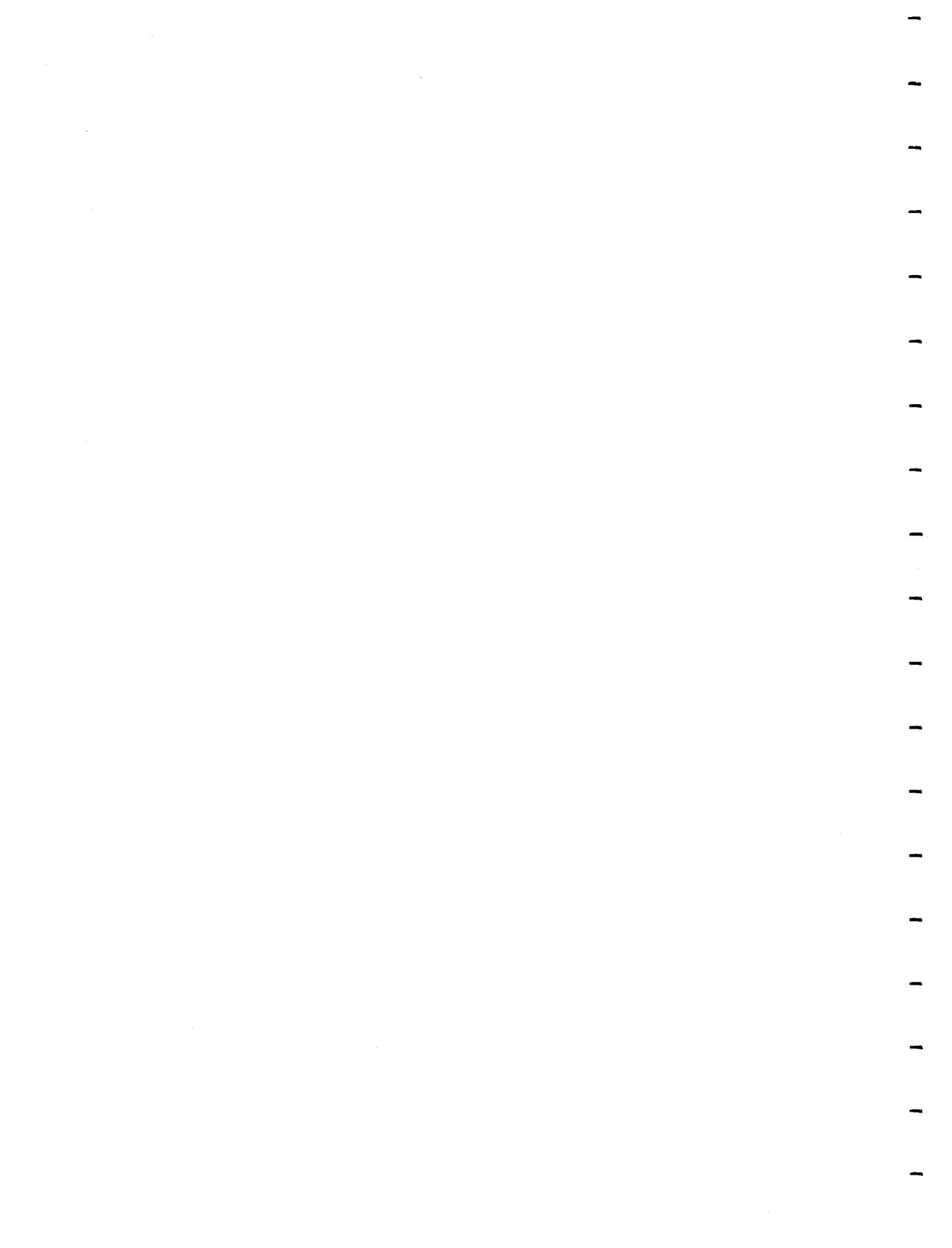
Al efectuar la verificación en el Departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, se determinó que no cuentan con un Plan de Continuidad del Negocio, (Business Continuity Planning -BCP-), a nivel de tecnología de la información, aprobado por la Dirección Ejecutiva en donde se detalle las actividades en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección Informática y Estadística. Así mismo al evaluar el Organigrama Institucional del Registro Nacional de las Personas -RENAP-, se observó que no se tiene implementada la figura de un Oficial de Seguridad Informático (OSI), que tenga a su cargo las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática.

En la Dirección de Procesos del Registro Nacional de las Personas -RENAP-, en el Departamento de Impresión, se determinó que la impresora DATACARD modelo MX6100, no es propiedad del Registro Nacional de las Personas y está en calidad de préstamo por parte de la empresa Entrust Datacard, la impresora anteriormente descrita se encuentra en desuso por generar manchas y puntos negros en el Documento de Identificación Personal -DPI- desde el 16 de octubre de 2017. Además durante el período de la auditoría, las impresiones del Documento de Identificación Personal -DPI-, eran realizadas por la empresa Easy Marketing S.A., la cual estaba certificada con la Norma ISO 9001, sobre la calidad de la gestión de la calidad. Así mismo en dicho Departamento, utilizan el sistema VPHOTO el cual es propiedad de la empresa Easy Marketing S.A.

En el Departamento de Control y Calidad, se observó que el ingreso al área restringida, donde están físicamente los Documentos de Identificación Personal -DPI- ya impresos, no cumple con las siguientes medidas de seguridad mínimas:

1. No existe una puerta que aisle la unidad catalogada como área restringida.
2. No cuentan con cámaras de circuito cerrado.





3. Carecen de extintores en el área, y en el lugar tienen cajas de cartón, cajas plásticas y bolsas plásticas, para el empaque de los Documentos de Identificación Personal -DPI's-.
4. Los Documentos Personales de Identificación no se resguardan en una caja de seguridad.

Además en el sistema de Impresión CIMCOR, que es el sistema utilizado para la impresión de los Documentos de Identificación Personal -DPI's- no existe la opción dentro del sistema, donde el analista consigne la cantidad de Documento de Identificación Personal -DPI- que ha recibido del coordinador para empezar el proceso de impresión por lotes.

Conclusiones

Se determinó que existen impresoras conectadas a la red institucional del Registro Nacional de las Personas -RENAP-, en las cuales el usuario administrador no está protegido con una contraseña asignada.

Se observó la existencia de puertos innecesarios activados en las impresoras, sin que exista control sobre los mismos.

Se determinó que no cuentan con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible, lo que origina que sea vulnerable a ataques de denegación de servicios (DoS).

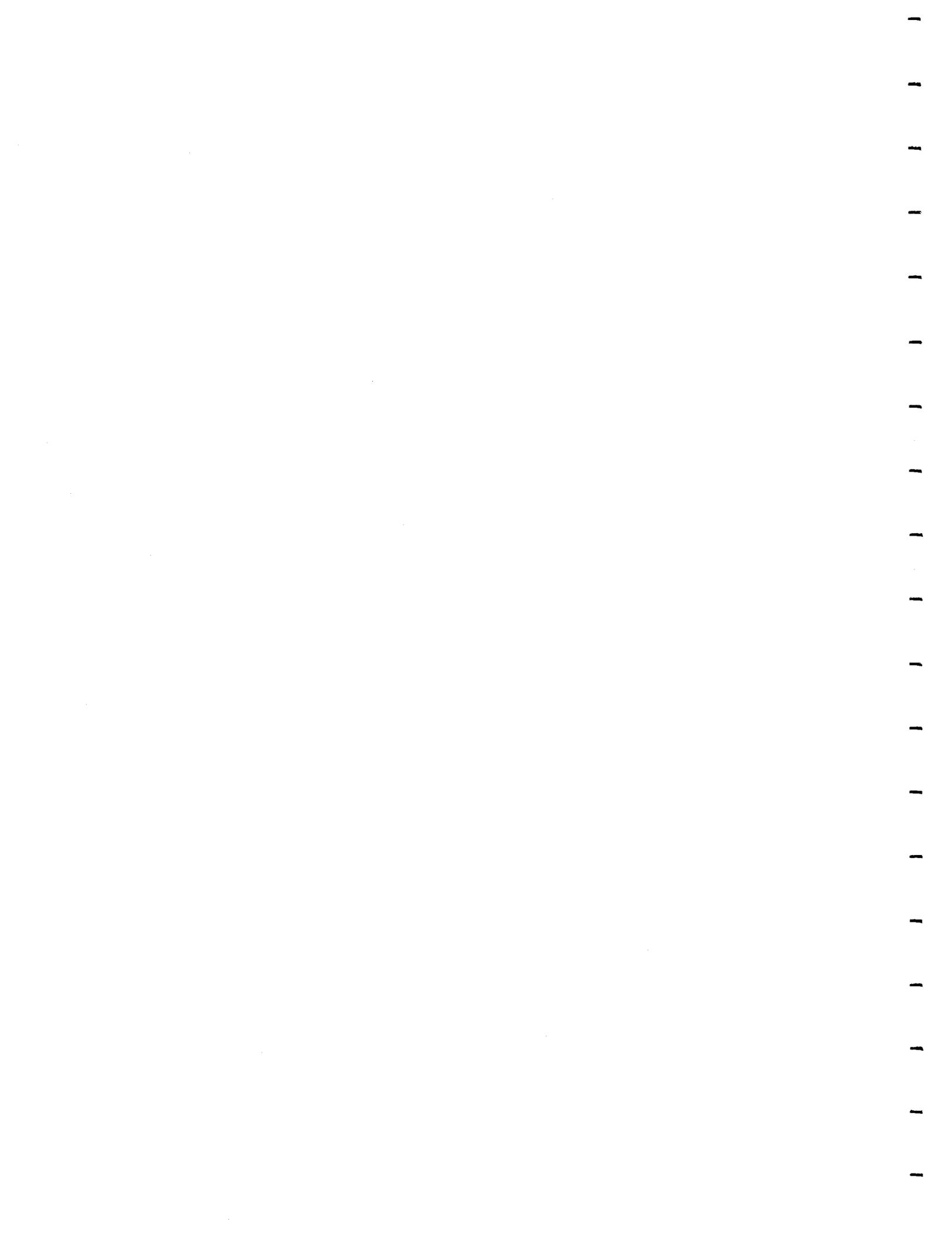
Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar suplantación de identidad (phishing), con la imagen de la institución. Por lo que se procedió a formular el hallazgo No. 1 del Área del Especialista de Control Interno. Vulnerabilidad en la Seguridad de los Servicios de la Red Interna.

Se determinó en el Departamento de Administración de Base de Datos, las siguientes deficiencias:

Actualmente tiene permisos, privilegios y acceso al módulo de Auditoría de la base de datos, denominado AUDIT_TRAIL, el Administrador de la Base de Datos (DBA).

No existe un procedimiento definido en el cual los cambios a la información de la base de datos solicitados por medio de oficio por el dueño de la información, se realicen en presencia del solicitante y dicho procedimiento quede plasmado en





Acta Administrativa. Por lo que se procedió a formular el hallazgo No. 2 del Área del Especialista de Control Interno. Falta de Procedimientos Para el Uso de Bitácoras.

Se estableció que en el Registro Nacional de las Personas -RENAP-, se carece de procedimientos y de una plataforma en donde se puedan efectuar los escenarios de prueba, para la actualización de Parches, que sirven para prevenir cualquier vulnerabilidad que afecte al sistema gestor de la base de datos. Por lo que se procedió a formular el hallazgo No. 3 del Área del Especialista de Control Interno. Desactualización de los Parches en la Base de Datos.

Se estableció que en el Departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, no cuentan con un Plan de Continuidad del Negocio (Business Continuity Planning -BCP-) a nivel de tecnología de la información, aprobado por la Dirección Ejecutiva en donde se detalle las actividades en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección de Informática y Estadística. Por lo que se procedió a formular el hallazgo No. 4 del Área del Especialista de Control Interno. Falta de un Plan de Continuidad del Negocio -BCP-.

Se observó que en el Registro Nacional de las Personas -RENAP-, dentro del Organigrama Institucional del RENAP, no se tiene implementada la figura de un Oficial de Seguridad Informático (OSI), que tenga a su cargo las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática. Por lo que se procedió a formular el hallazgo No. 5 del Área del Especialista de Control Interno. Falta de un Oficial de Seguridad.

En el Registro Nacional de las Personas -RENAP-, no se cuenta con las medidas de seguridad mínimas en el ingreso al área restringida del Departamento de Control de Calidad, en donde se resguardan físicamente los Documentos de Identificación Personal -DPI- ya impresos, determinándose las deficiencias siguientes:

- a. No se cuenta con una puerta que aisle la unidad catalogada como área restringida, únicamente se observaron rótulos impresos en donde se prohíbe el ingreso.
- b. No tienen suficientes cámaras de circuito cerrado de televisión -CCTV-, que permita monitorear las operaciones y al personal de la unidad de control de calidad. Únicamente se cuenta con una cámara fija.
- c. Carecen de extintores en el área, no obstante que trabajan con material inflamable (cajas de cartón, cajas plásticas y bolsas plásticas de empaque para los





DPI).

d. No se cuenta con una caja de seguridad, en donde se resguarden los Documentos de Identificación Personal -DPI- impresos. Por lo que se procedió a formular el hallazgo No. 6 del Área del Especialista de Control Interno. Falta de Seguridad y Condiciones Apropriadas en el Área de Trabajo.

Se observó que en el Departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, no existe un Sistema Formal de Nóminas y que durante los 10 años que tiene el RENAP de estar funcionando, la nómina de empleados (2,256 empleados) se registra en hojas de cálculo de Excel, las cuales son vulnerables y no presentan seguridad e integridad en el manejo de información de pago de las nóminas del personal. Por lo que se procedió a formular el hallazgo No. 7 del Área del Especialista de Control Interno. Falta de Sistema de Nóminas Para Administrar la Gestión de Recursos Humanos.

6. RESULTADOS DE LA AUDITORÍA

Hallazgos Relacionados con el Control Interno (Área Técnica)

Área Técnica

Hallazgo No. 1

Vulnerabilidad en la seguridad de los servicios de la red interna

Condición

En el Registro Nacional de las Personas -RENAP-, se efectuaron pruebas de escaneo en la red interna utilizando para el efecto herramientas tecnológicas, determinando las siguientes vulnerabilidades:

Equipos de impresión mal configurados

1. Se determinó que existen impresoras conectadas a la red institucional del RENAP, en las cuales el usuario administrador no está protegido con una contraseña asignada.
2. Se observó la existencia de puertos innecesarios activados en las impresoras, sin que exista control sobre los mismos.





Vulnerabilidad a ataques DoS y uso de imagen para Phishing

1. Se determinó que no se cuenta con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible lo que origina que sea vulnerable a ataques de denegación de servicios (DoS).
2. Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar phishing, con la imagen de la institución.

No se aplica Protocolos de seguridad HTTPS, en los Formularios de solicitud de información del portal web.

Dentro del Sitio Web de la Institución, existen 2 formularios para poder realizar consultas, los cuales no cuentan con un protocolo de seguridad -HTTPS-, que garantice el envío de la información cifrada.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.6, Tipos de Controles, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, establecer e implementar con claridad los diferentes tipos de control que se relacionan con los sistemas administrativos y financieros. En el Marco Conceptual de Control Interno Gubernamental, se establecen los distintos tipos de control interno que se refiere a: Control Interno Administrativo y Control Interno Financiero, y dentro de estos, el control previo, concurrente y posterior".

Causa

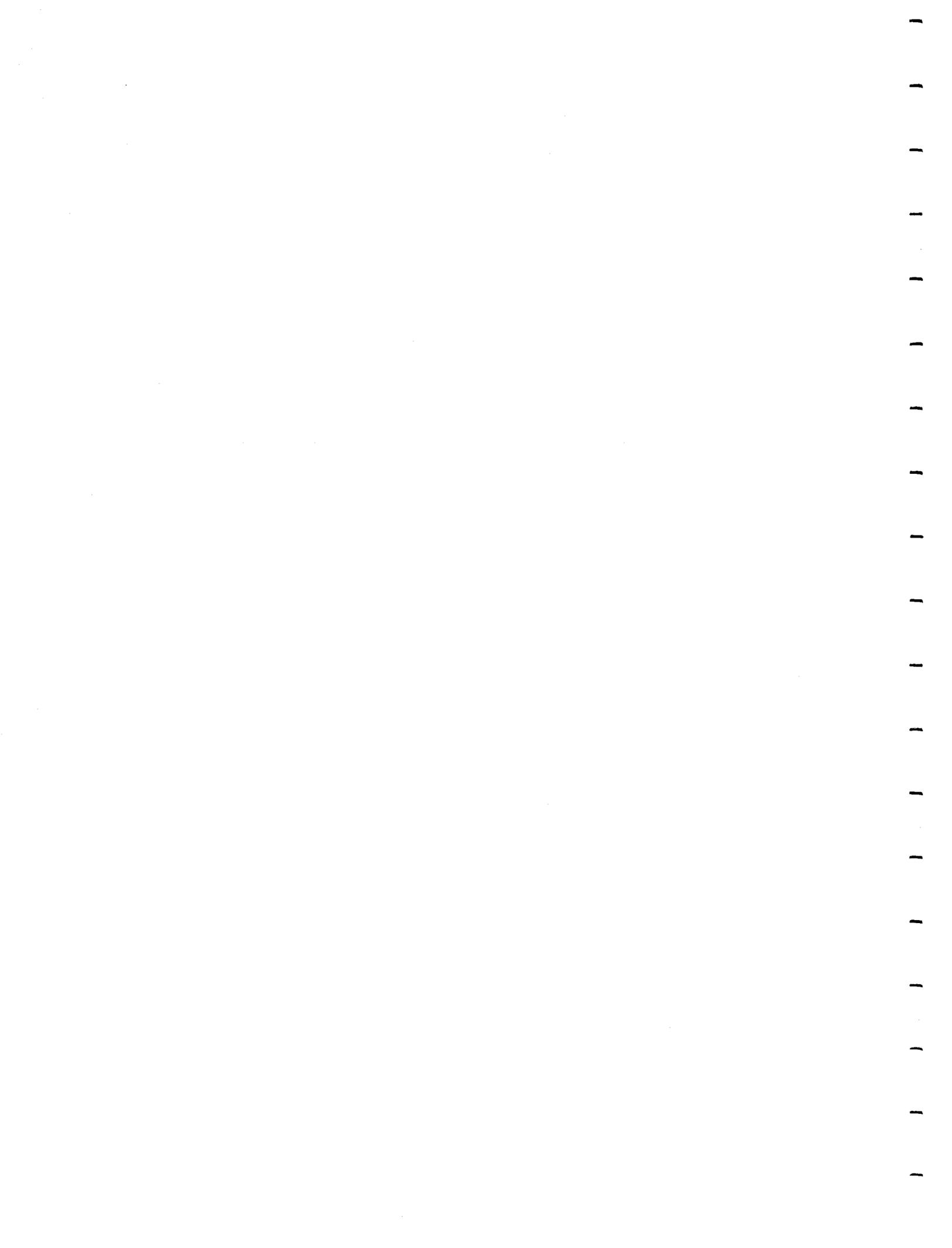
El Director de Informática y Estadística, el Sub Director de Servicios Críticos y el Jefe de Seguridad Informática, no han efectuado las verificaciones para que exista una adecuada configuración a los dispositivos de la red, códigos HTML, scripts utilizados en el Portal Web y protocolos de seguridad HTTPS, para garantizar el control y seguridad de los datos.

Efecto

Riesgo de ingreso a las consolas de administración por usuarios no autorizados y se efectúen cambios que provoquen que las impresoras dentro de la Red queden inhabilitadas.

Riesgo que el Portal Web, no se encuentre disponible, por ataques de denegación de servicios (DoS).





Riesgo que la imagen institucional plasmada en el sitio web sea utilizada por terceras personas para la práctica de phishing.

Riesgo que la información enviada a través de los formularios no cuenta con un certificado de HTTPS y viaje por la Internet sin cifrarse, la cual pueda ser utilizada por terceras personas.

Recomendación

El Director Ejecutivo debe girar sus instrucciones al Director de Informática y Estadística y este a su vez al Jefe y técnico encargado de la seguridad en el Departamento de Seguridad Informática, para que se efectúen las acciones necesarias para garantizar que las impresoras no queden inhabilitadas, la imagen institucional, la información administrada por los formularios del portal web sean utilizadas por terceras personas, así como la disponibilidad de dicho Portal.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Héctor Iván García Solórzano, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período comprendido del 01 de enero de 2015 al 31 de octubre de 2016, expone lo siguiente: "Yo, Héctor Iván García Solórzano, identificándome con DPI 2220 38918 0101 respetuosamente comparezco ante esta entidad contralora a evacuar la audiencia conferida y en consecuencia; hago constar que estuve en el cargo como subdirector de Servicios Críticos del 01 de julio de 2015 al 31 de marzo del 2016, presentando mi renuncia al puesto a la Dirección Ejecutiva el 28 de marzo de 2016, y se acepta mi renuncia el 31 de marzo de 2016 mediante oficio DA-SHR-dg-576-2016, haciendo constar que durante 8 meses de ocupar el puesto fue muy corto para poder evaluar y ejercer control en la subdirección de Servicios Críticos.

Vulnerabilidad en la seguridad de los servicios de la red interna.

Condición:

En el registro nacional de las Personas Renap, se efectuaron pruebas de escaneo en la red interna utilizando para el efecto herramientas tecnológicas, determinando las siguientes vulnerabilidades:

"Equipos de Impresión mal Configurados"

No tendría mayor impacto en la vulnerabilidad ya que las estaciones de trabajo se encontraban en el dominio y los puertos de los mismos se encontraban bloqueados. Durante el tiempo que asumí la subdirección así se encontró, esperando que en el término de este tiempo se haya mejorado





Vulnerabilidad a ataques DoS y uso de imagen para Phishing

Proyectado para el mes de julio la implementación. En el POA 2015.

No se aplica protocolos de seguridad HTTPS, en los formularios de solicitud de información del portal web.

Se compró certificado de dominio SSL en año 2015.

RAZONAMIENTO:

Proyecto la Jefatura de Seguridad Informática la solución IPS (Intrusion Prevention System), en el POA presentado del año 2015 área el mes de julio, el cual no fue adquirido. Pero por las medidas administrativas adoptadas a en el mes de febrero 2016 en circular de 007-2016, seguramente la adquirieron después de ya no estar en la Subdirección.

CONCLUSIÓN:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número dos (2), respecto a la Vulnerabilidad en la seguridad de los servicios de la red interna", derivado a que si se contempló".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Manuel Alejandro Rímola Cordero, Jefe de Seguridad Informática del Registro Nacional de las Personas, durante el periodo del 16 de julio al 01 de enero del 2015, expone lo siguiente: "Dentro del Registro Nacional de las Personas -RENAP- existe una red informática en la cual se encuentran instaladas impresoras para el uso de las diferentes oficinas registrales y administrativas de la Institución. Al realizar la instalación de una impresora dentro de la red se asigna una dirección IP que permitirá que los usuarios puedan comunicarse con la impresora y así poder realizar las impresiones. Las impresoras predeterminadamente tienen un programa o página de administración, el cual es accesible desde de un explorador Web a través del puerto 80 ó HTTP. En este programa o página de administración es posible tener cierta configuración de la impresora, pero nunca limitar el acceso a impresión de parte de los usuarios, por lo que no representa un riesgo de seguridad para la utilización de las impresoras. Sin embargo a pesar de no ser un riesgo en la seguridad se tomaron las acciones para configurar las impresoras y restringir el acceso al programa o página de administración, este permiso únicamente a los técnicos del Departamento Soporte Técnico.

En oficio DIE-5026-2017, la Dirección de Informática y Estadística solicita al Departamento de Seguridad Informática haga entrega del Plan de Trabajo sobre las acciones realizadas por la Contraloría General de Cuentas -CGC- por medio de la Cédula de Observaciones con fecha 27 de diciembre de 2017; se da





respuesta por medio de oficio DIE-SSC-DSI-0061-2017 y se traslada el Plan de Trabajo del Departamento de Seguridad Informática. Por medio de oficio DIE-SSC-DSI-0066-2017 el Departamento de Seguridad Informática solicita reunión con personal de la Subdirección de Servicios Críticos y del Departamento de Soporte Técnico para la coordinación de acciones derivado de las Observaciones realizadas por la Contraloría General de Cuentas. El 11 de enero de 2018 se remitió Plan de Trabajo al Departamento de Soporte Técnico por medio de oficio DIE-SSC-DSI-009-2018. De acuerdo a este plan, el Departamento de Soporte Técnico realizó las actividades encaminadas a asegurar la configuración de las impresoras conectadas a la red del Registro Nacional de las Personas -RENAP- activando un usuario y contraseña para el programa o página web de administración que por defecto tienen configuradas las impresoras, lo cual quedo establecido en el Informe "Acceso a Configuración de Impresoras conectas a la Red" fechado Febrero 2018 y recibido en fecha 20 de febrero de 2018 por la Dirección de Informática y Estadística. Cabe mencionar que por ser un programa o página Web de administración predeterminado en las impresoras no se puede desinstalar o bloquear de las mismas, y la única opción para proteger el acceso al mismo es colocar un usuario y contraseña.

Vulnerabilidad de ataques DoS y uso de imagen para Phishing

Se determinó que no se cuenta con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible lo que origina que sea vulnerable a ataques de denegación de servicios (DoS).

Todos los sitios de Web publicados están expuestos a amenazas y ataques de parte de personas malintencionadas o hackers, con el objetivo de extraer información crítica o dejar sin los servicios a los visitantes de dichos sitios. Todos los días los hackers prueban y utilizan nuevos métodos de ataque, incluso utilizan métodos más antiguos que siguen teniendo éxito en sus objetivos. Derivado de estos diversos ataques no es imposible poder garantizar en un 100% la seguridad de cualquier sitio publicado en la Web. Sin embargo es posible mitigar las posibilidades de éxito de estos ataques mediante la implementación de equipos o herramientas que permitan bloquear estos ataques. La Dirección de Informática y Estadística consciente de esta problemática ha solicitado en varias ocasiones, a través del Departamento de Seguridad Informática, la compra de dispositivos de seguridad que permitan realizar esta mitigación. Con el objetivo de contar con estos equipos dentro del Plan Operativo Anual -POA- de la Dirección, se incluyó la compra de un sistema de prevención de intrusos (IPS por sus siglas en inglés), el cual tiene como objetivo el control de acceso de la red y proteger a los sitios de ataques y abusos. Esta compra fue incluida en el POA y Anteproyecto de Presupuesto del año 2016, el cual fue trasladado mediante oficio DI-252-2014; se detalla en la página 4 del POA y en la página 7 del Anteproyecto de Presupuesto,





renglón 328 "Equipo renovado para mejora de seguridad y prevención de ataques - Mejoras en servicios internos de la institución", que hace referencia al POA. También fue incluido en Plan Anual de compras (PAC) del año 2017, el cual fue trasladado por medio de Oficio DI-4933-2016, ANEXO IV, Segundo Cuadro "SEGUNDO CUATRIMESTRE (MAYO- AGOSTO2017), No. 1. A pesar de haber sido solicitado no fue incluido en los presupuestos finales correspondientes. En el año 2018 se inicio el proceso de compra del equipo de seguridad IPS, el cual fue solicitado por medio de Requisición de Compra o Contrataciones No. RCC 000198 y actualmente se encuentra en etapa de aprobación de documentación.

Aunado a las gestiones de compra para este equipo, la Dirección de Informática y Estadística ha tomado acciones para la mitigación de ataques de denegación de servicios a nivel de host, como lo indica el informe "IMPLEMENTACION INFORMATICA PARA MITIGAR ATAQUES DE DENEGACION DE SERVICIO A NIVEL DE HOST" presentado en conjunto a la Dirección, por los Departamentos de Desarrollo de Sistemas y de Infraestructura Informática. En dicho informe se detalla la implementación de una herramienta para la prevención de intrusos, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta. Esto en respuesta al oficio DIE-SSC-DSI-0065-2017, en el cual se convocó a dichos Departamentos a reunión de coordinación para tomar las acciones pertinentes. Otra acción tomada fue fortalecer la configuración de una herramienta IPS que se encuentra implementado como parte del UTM (gestión unificada de amenazas, por sus siglas en inglés) del equipo de seguridad cortafuegos (firewall) perimetral, según consta en oficio DIE-SSC-DSI-0073-2018.

Asimismo, el Departamento de Seguridad Informática realizó las gestiones para la contratación de un servicio para la mitigación de ataques de negación de servicios (DDoS por sus siglas en inglés), el cual fue solicitado por medio de Requerimiento de Compra o Contrataciones de Servicio No. 00849, "Protección de Ataques contra Denegación de Servicio, que incluye cobertura de ataques en la capa de aplicación Web". Este servicio fue contratado mediante ACTA ADMINISTRATIVA NÚMERO CIENTO OCHENTA Y CUATRO GUION DOS MIL DIECIOCHO (184-2018) DE NEGOCIACION POR COMPRA DIRECTA DENOMINADA "SERVICIO DE PROTECCIÓN DE ATAQUES CONTRA DENEGACION DE SERVICIOS"; y fue implementado en el sitio Web de la institución a partir del 2 de noviembre de 2018.

2. Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar phishing, con la imagen de la institución.

El contenido de la página web siempre deberá ser público para que el explorador





del usuario lo pueda interpretar y pueda mostrarlo en el navegador del usuario. Para protección del contenido de la página se procedió a eliminar el clic derecho en la pantalla, sin embargo eso no garantiza que el usuario no pueda acceder al contenido de la página, en el caso de los script. El RENAP hace uso de un Sistema de Gestión de Contenidos (UTM, por sus siglas en inglés) el cual es un manejador de contenido conocido mundialmente y es utilizado por diferentes entidades, al cual únicamente se le agregan contenidos que deben de ser netamente públicos, por lo que no se ponen en riesgo la información interna del RENAP. Por lo tanto no se considera como una vulnerabilidad que el contenido de la página esté disponible para el usuario al dar clic secundario, pero como una buena práctica se procedió a eliminar dicha acción.

Aunado a esto, el RENAP cuenta con un certificado de seguridad SSL implementado en su dominio y subdominios lo cual garantiza al usuario final que todas las conexiones con la Institución son seguras.

No se aplica Protocolos de Seguridad HTTPS, en los Formularios de solicitud de información del portal Web.

La implementación de un certificado SSL sobre un dominio realiza la protección de todas y cada una de las páginas alojadas bajo el dominio protegido.

El dominio renap.gob.gt se encuentra protegido por un certificado SSL desde el año 2015 y los formularios indicados, como "sin protección" únicamente indicaban la advertencia sobre un link de una imagen con referencia a un link sin protocolo HTTPS y en ningún momento fue un formulario de captura de datos. Dicho link fue corregido por lo que la advertencia del certificado desapareció.

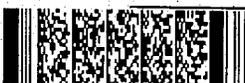
CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, solicito que se tenga por desvanecido el hallazgo número dos (2) de sistema de información deficiente, derivado a que en todo momento se han realizado gestiones y tomado acciones para la protección de la red y los sitios Web de la Institución, cumpliendo con la responsabilidad que correspondía a mi persona como Jefe de Seguridad Informática en Funciones en el período auditado.

PETICIONES:

Que se tenga por presentado en tiempo el presente memorial que contiene los argumentos legales y las pruebas de descargo correspondientes;

Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos el hallazgo números dos (2) relacionado, formulado hacia mi persona;





Que se me notifique de la resolución de desvanecimiento del referido hallazgo.

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Mónica Carolina Cárcamo Recinos, Jefe de Seguridad Informática del Registro Nacional de las Personas, durante el período del 02 de noviembre de 2015 al 04 de julio de 2016, expone lo siguiente: "Dentro del Registro Nacional de las Personas - RENAP- existe una red informática en la cual se encuentran instaladas impresoras para el uso de las diferentes oficinas registrales y administrativas de la Institución. Al realizar la instalación de una impresora dentro de la red se asigna una dirección IP que permitirá que los usuarios puedan comunicarse con la impresora y así poder realizar las impresiones. Las impresoras predeterminadamente tienen un programa o página de administración, el cual es accesible desde de un explorador Web a través del puerto 80 ó HTTP. En este programa o página de administración es posible tener cierta configuración de la impresora, pero nunca limitar el acceso a impresión de parte de los usuarios, por lo que no representa un riesgo de seguridad para la utilización de las impresoras. Sin embargo a pesar de no ser un riesgo en la seguridad se tomaron las acciones para configurarlas impresoras y restringir el acceso al programa o página de administración, este permiso únicamente a los técnicos del Departamento Soporte Técnico.

En oficio DIE-5026-2017, la Dirección de Informática y Estadística solicita al Departamento de Seguridad Informática haga entrega del Plan de Trabajo sobre las acciones realizadas por la Contraloría General de Cuentas -CGC- por medio de la Cédula de Observaciones con fecha 27 de diciembre de 2017; se da respuesta por medio de oficio DIE-SSC-DSI-0061-2017 y se traslada el Plan de Trabajo del Departamento de Seguridad Informática. Por medio de oficio DIE-SSC-DSI-0066-2017 el Departamento de Seguridad Informática solicita reunión con personal de la Subdirección de Servicios Críticos y del Departamento de Soporte Técnico para la coordinación de acciones derivado de las Observaciones realizadas por la Contraloría General de Cuentas. El 11 de enero de 2018 se remitió Plan de Trabajo al Departamento de Soporte Técnico por medio de oficio DIE-SSC-DSI-009-2018. De acuerdo a este plan, el Departamento de Soporte Técnico realizó las actividades encaminadas a asegurar la configuración de las impresoras conectadas a la red del Registro Nacional de las Personas -RENAP- activando un usuario y contraseña para el programa o página web de administración que por defecto tienen configuradas las impresoras, lo cual quedo establecido en el Informe "Acceso a Configuración de Impresoras conectas a la Red" fechado Febrero 2018 y recibido en fecha 20 de febrero de 2018 por la Dirección de Informática y Estadística. Cabe mencionar que por ser un programa o página Web de administración predeterminado en las impresoras no se puede desinstalar o bloquear de las mismas, y la única opción para proteger el acceso al mismo es colocar un usuario y contraseña.



Vulnerabilidad de ataques DoS y uso de imagen para Phishing

1. Se determinó que no se cuenta con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible lo que origina que sea vulnerable a ataques de denegación de servicios (DoS).

Todos los sitios de Web publicados están expuestos a amenazas y ataques de parte de personas malintencionadas o hackers, con el objetivo de extraer información crítica o dejar sin los servicios a los visitantes de dichos sitios. Todos los días los hackers prueban y utilizan nuevos métodos de ataque, incluso utilizan métodos más antiguos que siguen teniendo éxito en sus objetivos. Derivado de estos diversos ataques no es imposible poder garantizar en un 100% la seguridad de cualquier sitio publicado en la Web. Sin embargo es posible mitigar las posibilidades de éxito de estos ataques mediante la implementación de equipos o herramientas que permitan bloquear estos ataques. La Dirección de Informática y Estadística consciente de esta problemática ha solicitado en varias ocasiones, a través del Departamento de Seguridad Informática, la compra de dispositivos de seguridad que permitan realizar esta mitigación. Con el objetivo de contar con estos equipos dentro del Plan Operativo Anual -POA- de la Dirección, se incluyó la compra de un sistema de prevención de intrusos (IPS por sus siglas en inglés), el cual tiene como objetivo el control de acceso de la red y proteger a los sitios de ataques y abusos. Esta compra fue incluida en el POA y Anteproyecto de Presupuesto del año 2016, el cual fue trasladado mediante oficio DI-252-2014; se detalla en la página 4 del POA y en la página 7 del Anteproyecto del Presupuestos, renglón d 328 "Equipo renovado para mejora de seguridad y prevención de ataques - Mejoras en servicios internos de la institución", que hace referencia al POA. También fue incluido en Plan Anual de compras (PAC) del año 2017, el cual fue trasladado por medio de Oficio DI-4933-2016, ANEXO IV, Segundo Cuadro "SEGUNDO CUATRIMESTRE (MAYO- AGOSTO 2017), No. 1. A pesar de haber sido solicitado no fue incluido en los presupuestos finales correspondientes. En el año 2018 se inicio el proceso de compra del equipo de seguridad IPS, el cual fue solicitado por medio de Requisición de Compra o Contrataciones No. RCC 000198 y actualmente se encuentra en etapa de aprobación de documentación.

Aunado a las gestiones de compra para este equipo, la Dirección de Informática y Estadística ha tomado acciones para la mitigación de ataques de denegación de servicios a nivel de host, como lo indica el informe "IMPLEMENTACION INFORMATICA PARA MITIGAR ATAQUES DE DENEGACION DE SERVICIO A NIVEL DE HOST" presentado en conjunto a la Dirección, por los Departamentos de Desarrollo de Sistemas y de Infraestructura Informática. En dicho informe se detalla la implementación de una herramienta para la prevención de intrusos, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por



fuerza bruta. Esto en respuesta al oficio DIE-SSC-DSI-0065-2017, en el cual se convocó a dichos Departamentos a reunión de coordinación para tomar las acciones pertinentes. Otra acción tomada fue fortalecer la configuración de una herramienta IPS que se encuentra implementado como parte del UTM (gestión unificada de amenazas, por sus siglas en inglés) del equipo de seguridad cortafuegos (firewall) perimetral, según consta en oficio DIE-SSC-DSI-0073-2018.

Asimismo, el Departamento de Seguridad Informática realizó las gestiones para la contratación de un servicio para la mitigación de ataques de negación de servicios (DDoS por sus siglas en inglés), el cual fue solicitado por medio de Requerimiento de Compra o Contrataciones No. 00849, "Servicio de Protección de Ataques contra Denegación de Servicio, que incluye cobertura de ataques en la capa de aplicación Web". Este servicio fue contratado mediante ACTA ADMINISTRATIVA NÚMERO CIENTO OCHENTA Y CUATRO GUION DOS MIL DIECIOCHO (184-2018) DE NEGOCIACION POR COMPRA DIRECTA DENOMINADA "SERVICIO DE PROTECCIÓN DE ATAQUES CONTRA DENEGACION DE SERVICIOS", y fue implementado en el sitio Web de la institución a partir del 2 de noviembre de 2018.

2. Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar phishing, con la imagen de la institución.

El contenido de la página web siempre deberá ser público para que el explorador del usuario lo pueda interpretar y pueda mostrarlo en el navegador del usuario. Para protección del contenido de la página se procedió a eliminar el clic derecho en la pantalla, sin embargo eso no garantiza que el usuario no pueda acceder al contenido de la página, en el caso de los script. El RENAP hace uso de un Sistema de Gestión de Contenidos (UTM, por sus siglas en inglés) el cual es un manejador de contenido conocido mundialmente y es utilizado por diferentes entidades, al cual únicamente se le agregan contenidos que deben de ser netamente públicos, por lo que no se ponen en riesgo la información interna del RENAP. Por lo tanto no se considera como una vulnerabilidad que el contenido de la página esté disponible para el usuario al dar clic secundario, pero como una buena práctica se procedió a eliminar dicha acción.

Aunado a esto, el RENAP cuenta con un certificado de seguridad SSL implementado en su dominio y subdominios lo cual garantiza al usuario final que todas las conexiones con la Institución son seguras.

No se aplica Protocolos de Seguridad HTTPS, en los Formularios de solicitud de información del portal Web.





La implementación de un certificado SSL sobre un dominio realiza la protección de todas y cada una de las páginas alojadas bajo el dominio protegido.

El dominio renap.gob.gt se encuentra protegido por un certificado SSL desde el año 2015 y los formularios indicados, como "sin protección" únicamente indicaban la advertencia sobre un link de una imagen con referencia a un link sin protocolo HTTPS y en ningún momento fue un formulario de captura de datos. Dicho link fue corregido por lo que la advertencia del certificado desapareció.

CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, solicito que se tenga por desvanecido el hallazgo número dos (2) de sistema de información deficiente, derivado a que en todo momento se han realizado gestiones y tomado acciones para la protección de la red y los sitios Web de la Institución, cumpliendo con la responsabilidad que correspondía a mi persona como Jefe de Seguridad Informática en Funciones en el período auditado.

PETICIONES:

Que se tenga por presentado en tiempo el presente memorial que contiene los argumentos legales y las pruebas de descargo correspondientes;

Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos el hallazgo números dos (2) relacionado, formulado hacia mi persona;

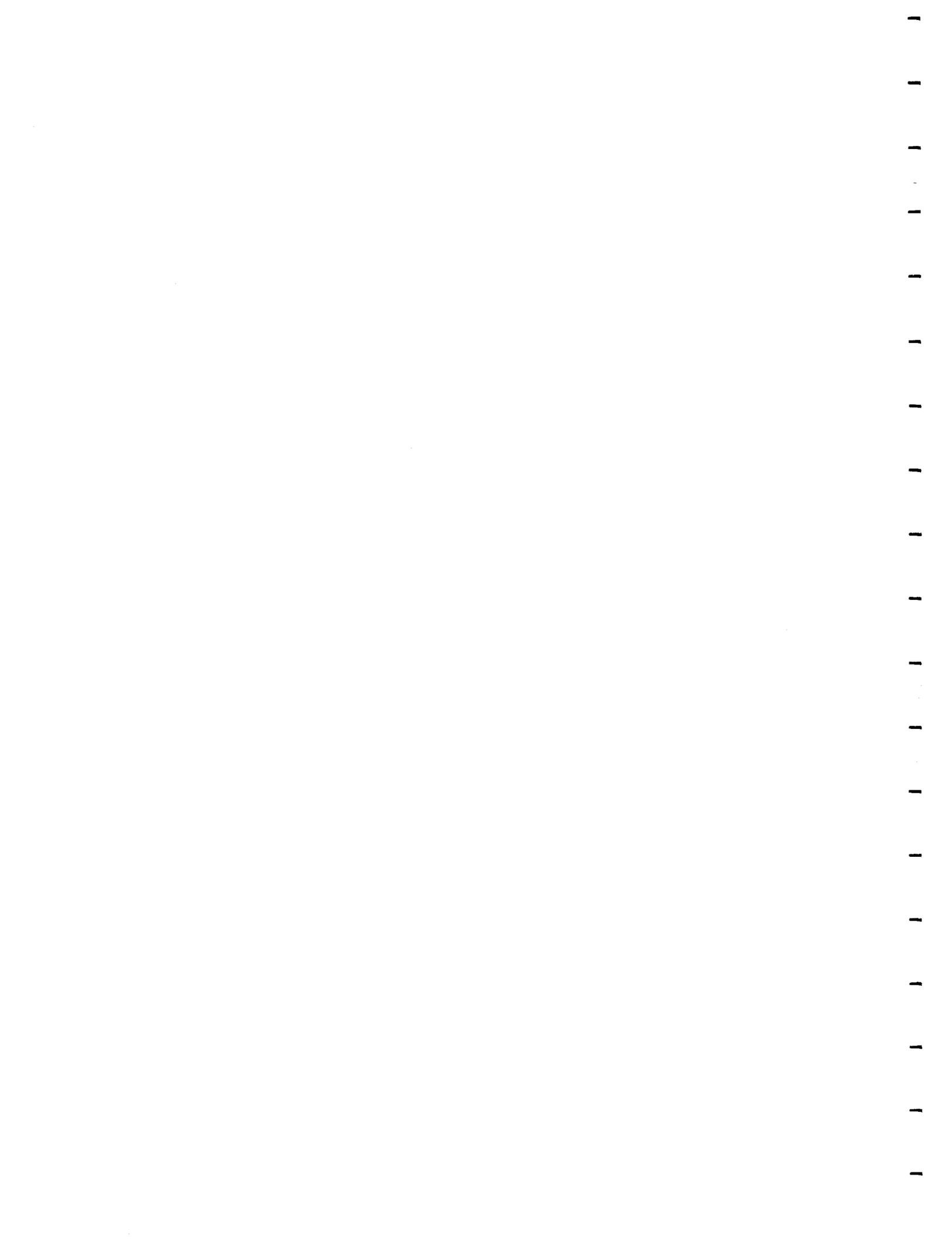
Que se me notifique de la resolución de desvanecimiento del referido hallazgo.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Omar Esduardo Sagastume Álvarez, Jefe de Seguridad Informática del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 15 de julio de 2015, expone lo siguiente: "Yo Omar Esduardo Sagastume Álvarez, de cuarenta y seis años de edad, casado, guatemalteco, Ingeniero en Sistemas de Información, respetuosamente me presento en la CGC para evacuar la audiencia de comunicación de resultados de 1 hallazgo de Control Interno. Hallazgo No. 2 Vulnerabilidad en la seguridad de los servicios de la red interna.

EXPONGO:

DE LA NOTIFICACIÓN. Con fecha 20 de diciembre de 2018, fui notificado del oficio número CGC-RENAP-019-2018 con fecha 17 de diciembre de 2018, mediante el cual se señala fecha para la discusión de hallazgos, para el miércoles 16 de enero de 2019, a las diez (10:00) horas, en las oficinas centrales de la Contraloría General de Cuentas, 4º Nivel Salón La Ceiba, para que presentar la documentación escrita y en forma magnética (formato Word o Excel, sin





contraseña) según corresponda, para someter a evaluación y análisis por parte del Equipo de Auditoría, por lo que al respecto expongo lo siguiente:

Que me retire de la institución el 15-7-2015.

Que con fecha 26 de diciembre del año 2018 solicite a la Unidad de Información Pública del Registro Nacional de las Personas, la información solicitada por la Contraloría General de Cuentas (Oficio no. CGC-RENAP-NOT-019-2018). De lo cual fui notificado vía correo electrónico de fecha 11 de enero del año 2019 a las 17:31 según Resolución UIP NO. 19-2019; al presentarme el día 14 de enero del 2019 me fue entregada constancia de relación laboral en la cual se hace constar que deje de laborar en la institución a partir del 16 de julio del 2015 por motivo de renuncia. Y que según Oficio DIE guión ciento treinta y tres guion dos mil diecinueve (OFICIO-DIE-133-2019) emitido por la Dirección de Informática y Estadística del Registro Nacional de las personas, en el cual indican que aun no se ha cumplido la fecha de comunicación de resultados de los hallazgos establecida por la Contraloría General de Cuentas y que por ende no se cuenta con lo solicitado "documentación para evaluación y análisis de desvanecimiento de hallazgos.

Derivado que a la fecha el RENAP no me ha proporcionado la información solicitada según lo expuesto en el numeral anterior, consulte la página web del RENAP sección de Información Pública ítem Organización, de lo cual reitero que:

Primero: Que en el POA_2015

EJE ESTRATEGICO 2 – REINGENIERÍA

Se le asigna a la Dirección de Informática y Estadística los siguientes objetivos:

Objetivo Operativo # 19

Implementar nuevas herramientas Informáticas

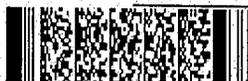
Objetivo Operativo # 22

Fortalecer el crecimiento en la prestación de servicios electrónicos

Para ello la Jefatura de Seguridad Informática dejo propuesto en el Plan Operativo Anual, POA-2015 # página 69 y 71

El Objetivo Operativo:

Brindar seguridad de acceso a los sistemas, servicios y aplicaciones.





Por medio de la actividad de:

Comprar 30 switch administrables

Implementar un correlacionador de eventos

Implementar un NAC (Network Access Control)

Implementar un IPS (Sistemas de Prevención de Intrusos) de zona

Las anteriores actividades resultarían en:

Tener una gestión adecuada de la LAN de la oficina central

Identificar Oportunamente Incidente y Ataques

Asegurar sistemas, servicios y aplicaciones

Resguardar sistemas, servicios y aplicaciones

Adicionalmente Procurar funcionamiento sin interrupción

Por medio de la actividad de:

Actualizar periódicamente el sitio web de RENAP

Conclusión: La Jefatura de Seguridad Informática si contemplo en el POA2015 las ejecuciones presupuestarias correspondientes a Seguridad y Control, sin embargo, no habían sido aprobadas o bien se encontraban en proceso de aprobación a la fecha de mi retiro de la institución el 15 de julio 2015.

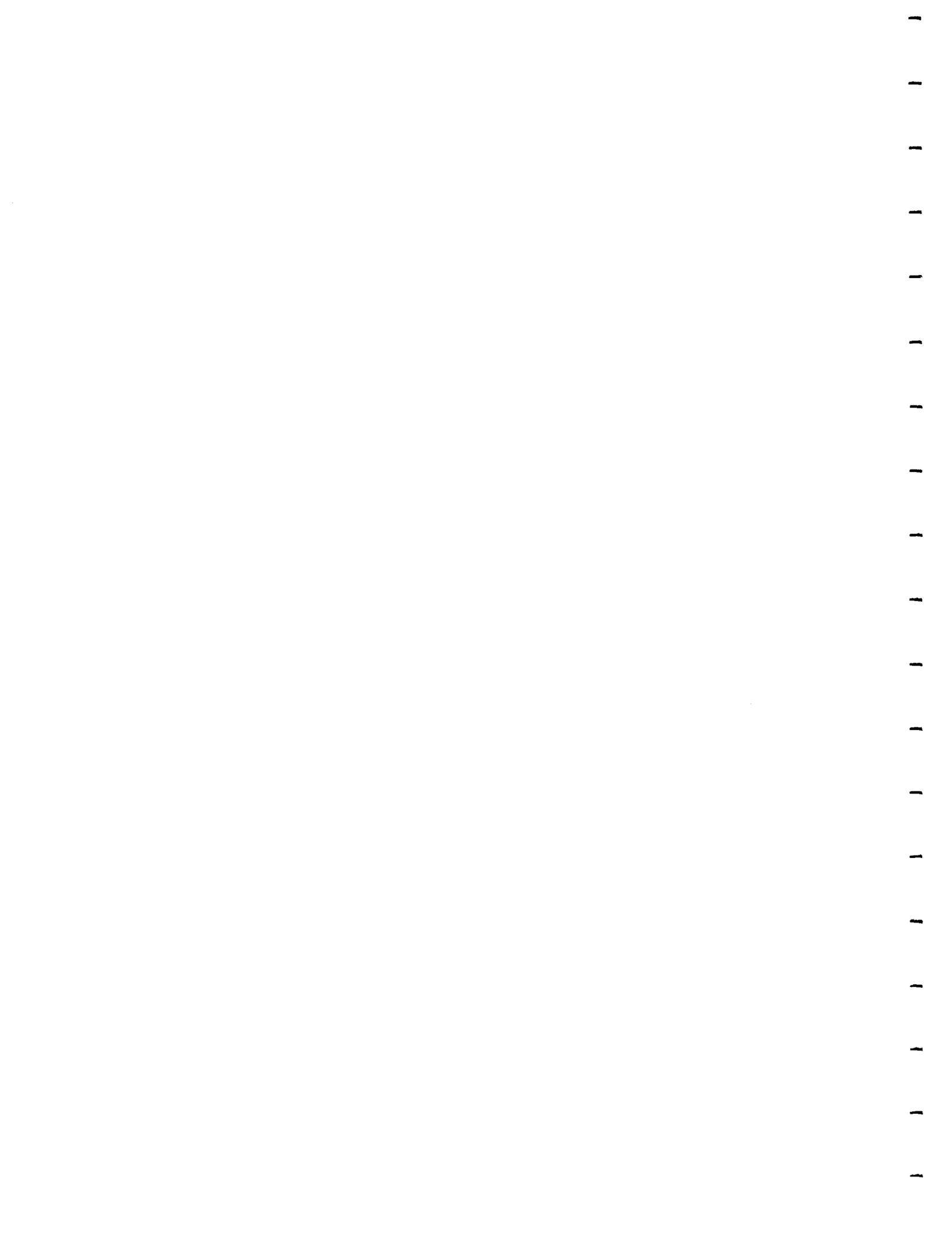
Segundo: En la causa del hallazgo indica una estructura Institucional vigente posterior a mi retiro de la institución, según Acuerdo de Directorio número 80-2016 páginas 23 a la 26 en dicho acuerdo que indica que el tema de seguridad es un tema integral de toda la Dirección de Informática y Estadística, subdirecciones y sus diversos departamentos y no competencia exclusiva del departamento de Seguridad Informática.

Tercero: Al consultar el ePortal del Renap se puede visualizar que se utiliza el protocolo HTTPS de igual forma Certificado de seguridad SSL (Secure Sockets Layer – Capa de Sockets Seguros) autentifica la identidad de un sitio web y cifra con tecnología SSL la información que se envía al servidor.

Cuarto: Solicito tener en consideración que de la auditoría en mención DAS-12-0009-2017 de fecha 18 de mayo 2017 (periodo de evaluación 1-1-2015 al 31-10-2016) no he tenido la oportunidad de una actividad previa de Discusión de hallazgos y Seguimiento de recomendaciones, según el Marco Conceptual de Auditoría Gubernamental de la Contraloría General de Cuentas – Normas para la Comunicación de Resultados (incisos 4.3. y 4.6)

Quinto: Referente a:





Equipos de impresión mal configurados

1. Se determinó que existen impresoras conectadas a la red institucional del RENAP, en las cuales el usuario administrador no está protegido con una contraseña asignada.
2. Se observó la existencia de puertos innecesarios activados en las impresoras, sin que exista control sobre los mismos.

Durante el proceso de instalación de una impresora dentro de la red se asigna una dirección IP que permite a los usuarios comunicarse con la impresora y realizar impresiones. De forma predeterminada las impresoras tienen un programa o página de administración, accesible desde un explorador Web por el puerto 80 ó HTTP. En este software de administración es posible realizar la configuración de la impresora, pero nunca limitar el acceso a impresión, por lo que no representa un riesgo de seguridad para la utilización de las impresoras. A pesar de no ser un riesgo en la seguridad se toman acciones para configurar las impresoras y restringir el acceso al software de administración (el cual no es posible desinstalar por ser inherente a las impresoras), el acceso solo es posible solo utilizando usuario y contraseña por el personal del Departamento Soporte Técnico del RENAP.

Vulnerabilidad a ataques DoS y uso de imagen para Phishing

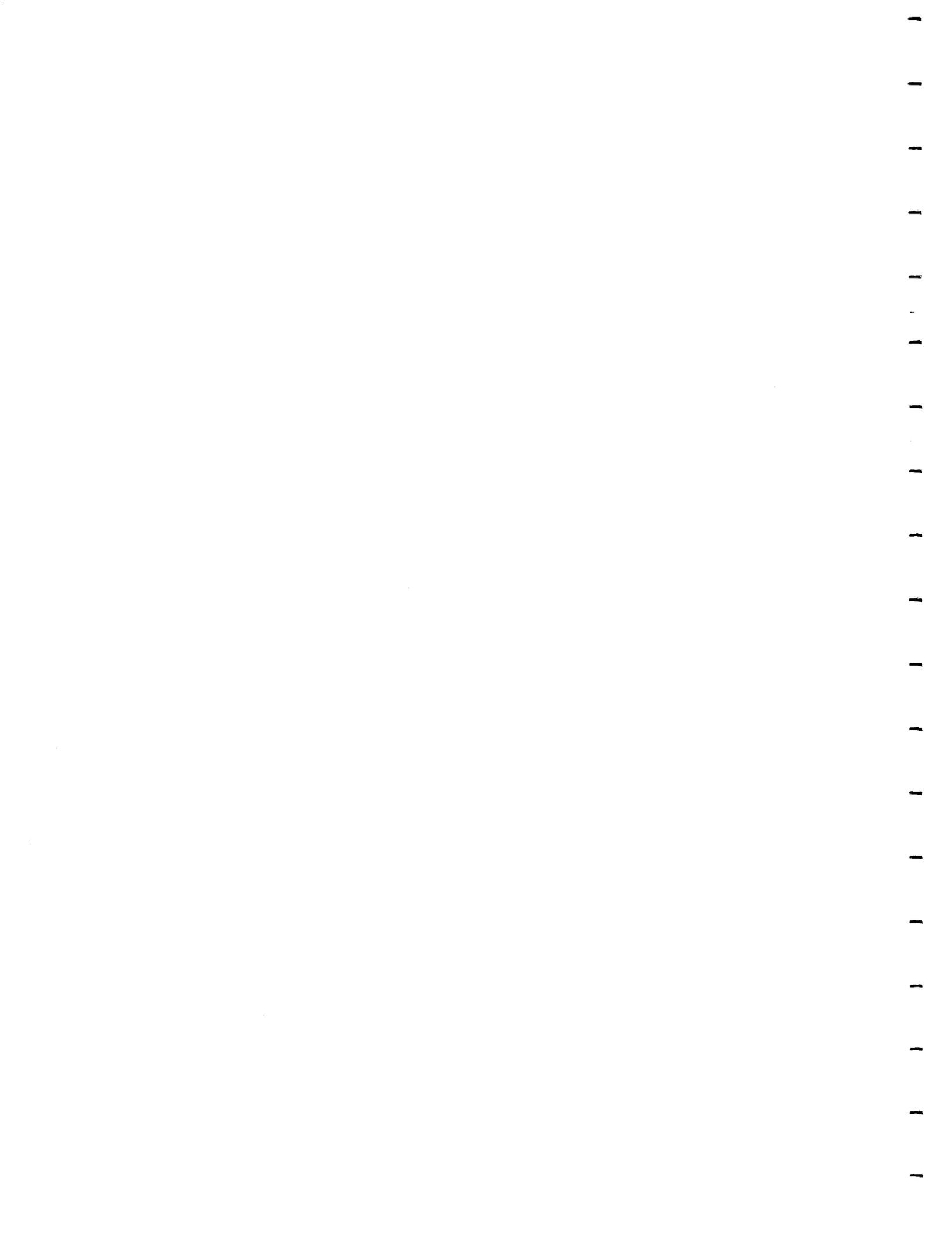
1. Se determinó que no se cuenta con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible lo que origina que sea vulnerable a ataques de denegación de servicios (DoS).

Todos los servicios publicados en la Web son sujetos de amenazas y ataques de hackers, con la finalidad de generar irregularidad en los servicios o afectar la información de dichos sitios. Estas formas de ataque evolucionan constantemente. Por lo que no un método o herramienta para garantizar un nivel de seguridad al 100% en las plataformas de la web. Existe la posibilidad de mitigar o gestionar los riesgos de ataque por medio de la implementación de herramientas de software o equipos que permitan bloquear dichos ataques.

Durante mi gestión en la Jefatura de Seguridad Informática se solicitó por medio de la Dirección de Informática y Estadística, la compra de herramientas de seguridad que permitieran realizar acciones de mitigación de ataques; dichas iniciativas fueron plasmadas en el Plan Operativo Anual -POA- de la Dirección, donde fue incluida la compra de un sistema de prevención de intrusos (IPS), witchs administrables como objetivo el control de acceso de la red y proteger los servicios de red interna y externa.

De igual forma como iniciativa para la mitigación de ataques de denegación de servicios a nivel de host en el POA 2015, se indica la implementación de una





herramienta para la prevención de intrusos que bloquea las conexiones remotas que intentan accesos no autorizados, como lo indica el informe "IMPLEMENTACION INFORMATICA PARA MITIGAR ATAQUES DE DENEGACION DE SERVICIO A NIVEL DE HOST, dicha herramienta debía ser gestionada en conjunto a las directrices de la Dirección de Informática y Estadística, por los Departamentos de Desarrollo de Sistemas y Departamento de Infraestructura.

Adicionalmente en el POA 2015 se indica fortalecer la seguridad por medio de la herramienta IPS en conjunto con la actualización del cortafuegos perimetral (firewall). También se solicitó la implementación de un servicio tercerizado de protección de ataques informáticos.

2. Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar phishing, con la imagen de la institución.

Dentro del el contenido de la página web siempre deberá ser público para que el explorador del usuario lo pueda interpretar y pueda mostrarlo en el navegador del usuario, y se procedió a eliminar el clic derecho en la pantalla, sin embargo eso no garantiza que el usuario no pueda acceder al contenido de la página, en el caso de los script y hoja de estilos también es posible realizar modificaciones lo cual ayuda la utilización de los mismos, RENAP hace uso de un CMS el cual es un manejador de contenido conocido mundialmente y es utilizado por diferentes entidades, al cual únicamente se le agregan contenidos que deben de ser netamente públicos, por lo que no se ponen en riesgo la información interna del RENAP, aplicar modificaciones a un CMS. Por lo tanto, no se considera como una vulnerabilidad que el contenido de la página esté disponible para el usuario al dar clic secundario, pero como una buena práctica se procedió a eliminar dicha acción. Adicionalmente el RENAP cuenta con un certificado SSL implementado en su dominio y subdominios lo cual garantiza al usuario final que todas las conexiones con la Institución son seguras.

No se aplica Protocolos de Seguridad HTTPS, en los Formularios de solicitud de información del portal Web.

La implementación de un certificado SSL sobre un dominio realiza la protección de todas y cada una de las páginas alojadas bajo el dominio protegido. El dominio renap.gob.gt se encuentra protegido por un certificado SSL desde el año 2015 y los formularios indicados, como sin protección únicamente indicaban advertencia sobre un link de una imagen que hacía un link sin protocolo HTTPS y en ningún momento fue un formulario de captura de datos.





CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, solicito que se tenga por desvanecido el hallazgo número dos (2) de sistema de información deficiente, derivado a que en todo momento se han realizado gestiones y tomado acciones para la protección de la red y los sitios Web de la Institución, cumpliendo con la responsabilidad que correspondía a mi persona como Jefe de Seguridad Informática en Funciones en el período auditado.

PETICIONES:

Que se tenga por presentado en tiempo lo solicitud realizadas por la CGC que contiene los argumentos legales y las pruebas de descargo correspondientes.

Que se considera que el Registro Nacional de las Personas no me proporciono información documentada previo a esta audiencia, lo cual fue solicita con la debida anticipación y por medio de los medios legales correspondientes (Unidad de Información Pública del RENAP).

Que se consideren a mí favor las pruebas de descargo que presenten las otras personas a las que se le vinculo el mismo hallazgo (no. 2) y que el RENAP si les proporciono documentación para el desvanecimiento del hallazgo.

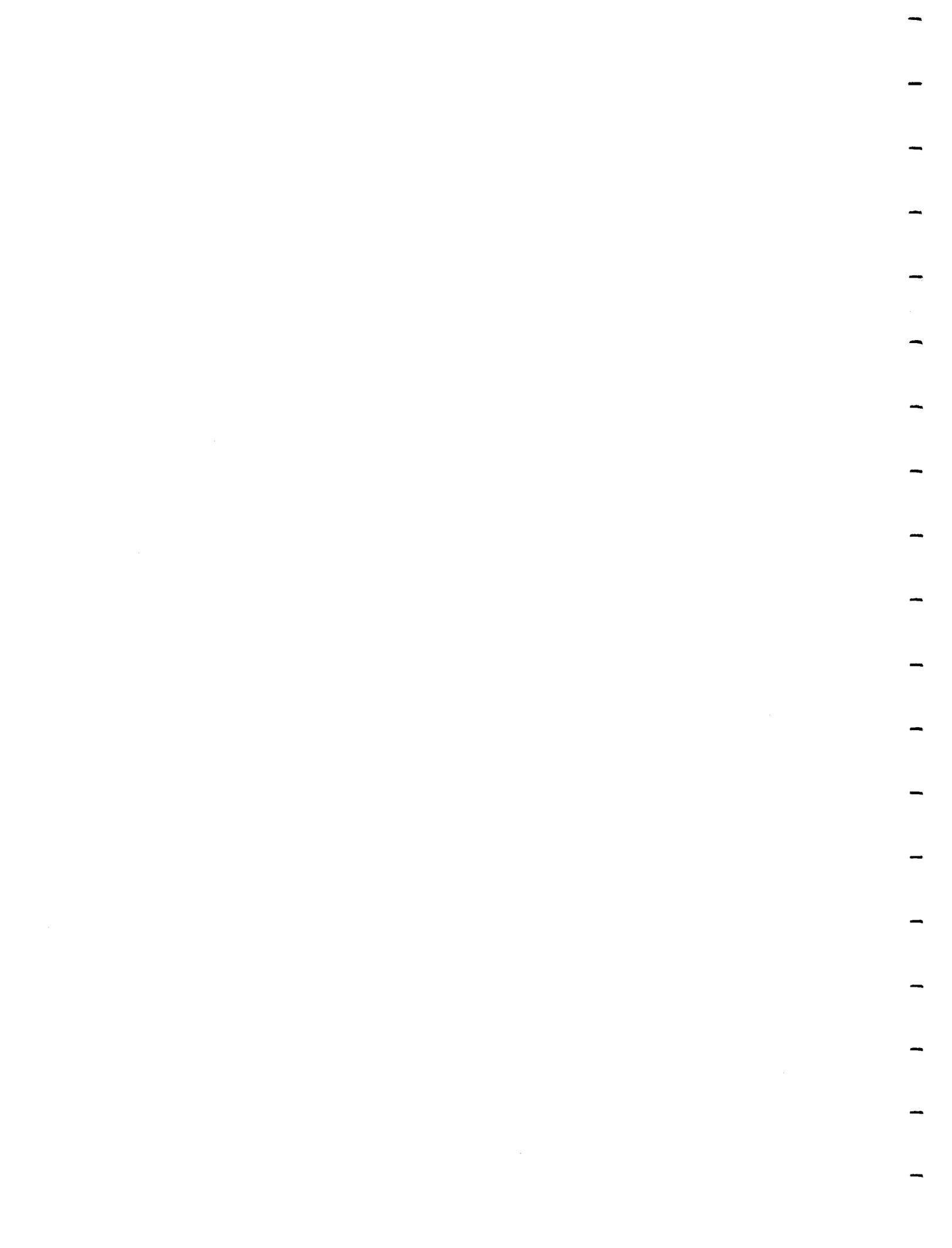
Se proceda con la evaluación descargo y desvanecimiento del hallazgo números dos (2) relacionado, formulado hacia mi persona y se proceda con la notificación escrita que acredite el desvanecimiento del referido hallazgo”.

Mediante oficio s/n y sin fecha, el señor Carlos Alberto Quintana Galindo, Director de Informática y Estadística del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 31 de octubre de 2016, indica lo siguiente: “En cuanto a la vulnerabilidad y seguridad se realizaron los esfuerzos para incorporar tecnologías que permitieran al departamento de seguridad tener ips (Intrusion Prevention System), sin embargo los procesos de adquisición suspendidos durante el 2016, afectaron dicha incorporación, que finalmente se realizó.

Si se cuenta con el protocolo https y cubre todo el dominio Renap.gob.gt, en el caso de los formularios se dio el caso que el link se encontraba mal re direccionado y no tenía incidencia en la seguridad que proporciona a todo el sitio el certificado de seguridad.

Así mismo el Renap cuenta con la administración active directory de usuarios, entre otras acciones proteger de vulnerabilidades locales que se puedan presentar.





PETICION:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número dos (2); respecto a la Vulnerabilidad en la seguridad de los servicios de la red interna.

Comentario de la Auditoría

Se desvanece el presente hallazgo para el señor Héctor Iván García Solorzano, quién fungió como Subdirector de Servicios Críticos del Registro Nacional de las Personas, por el período del 01 de enero de 2015 al 31 de octubre de 2016, ya que al analizar las pruebas de descargo presentadas se evidencia que realizó gestiones durante el período del 01 de julio 2015 al 31 de marzo de 2016, en el que ejerció funciones, para mejorar los aspectos de vulnerabilidad en la seguridad.

Se confirma el presente hallazgo para el señor Omar Esduardo Sagastume Alvarez, quién fungió como Jefe de Seguridad Informática del Registro Nacional de las Personas por el período del 01 de enero de 2015 al 31 de octubre de 2016; al señor Manuel Alejandro Rimola Cordero, quién fungió como Jefe de Seguridad Informática del Registro Nacional de las Personas por el período del 16 de julio al 01 de noviembre de 2015 y para la señora Mónica Carolina Cárcamo Recinos, quién fungió como Jefe de Seguridad Informática del Registro Nacional de las Personas, durante el período del 02 de noviembre de 2015 al 04 de julio de 2016; ya que al analizar las pruebas de descargo presentadas, analizar el Plan Operativo Anual del año 2015 y otras gestiones realizadas, mediante las pruebas de auditoría, se evidencia que al realizar la instalación de las impresoras en red no se estableció un usuario y contraseña para acceder a la configuración del equipo, no se presentaron las justificaciones necesarias de los puertos abiertos, así mismo se evidencia que las acciones correctivas se realizaron después del período auditado.

Se confirma el presente hallazgo para el señor Carlos Alberto Quintana Galindo, quién fungió como Director de Informática y Estadística, durante el período del 01 de enero de 2015 al 31 de octubre de 2016; ya que al analizar las pruebas de descargo presentadas se determinó que no se tomaron las acciones oportunas para poder establecer las configuraciones que permitieran mejorar la seguridad de los servicios de impresión en red, direccionar adecuadamente las páginas dentro del dominio de la entidad, así mismo se evidencia que las acciones correctivas se realizaron después del período auditado.

Este hallazgo fue notificado con el número 2 y corresponde en el presente informe al número 1.

Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la





República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
JEFE DE SEGURIDAD INFORMATICA	MANUEL ALEJANDRO RIMOLA CORDERO	4,500.00
DIRECTOR DE INFORMATICA Y ESTADISTICA	CARLOS ALBERTO QUINTANA GALINDO	7,500.00
JEFE DE SEGURIDAD INFORMATICA	OMAR ESDUARDO SAGASTUME ALVAREZ	4,500.00
JEFE DE SEGURIDAD INFORMATICA	MONICA CAROLINA CARCAMO RECINOS	4,500.00
Total		Q. 21,000.00

Hallazgo No. 2

Falta de procedimientos para el uso de bitácoras

Condición

En el Registro Nacional de las Personas -RENAP-, se observó que actualmente tiene acceso el Administrador de la Base de Datos (DBA), al módulo de Auditoría de la base de datos, denominado AUDIT_TRAIL.

Además se determinó que no existe un procedimiento definido en el cual los cambios a la información de la Base de Datos solicitados por oficio por el dueño de la información, se realicen en presencia del solicitante y dicho procedimiento quede plasmado en Acta Administrativa.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.6, Tipos de Controles, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, establecer e implementar con claridad los diferentes tipos de control que se relacionan con los sistemas administrativos y financieros. En el Marco Conceptual de Control Interno Gubernamental, se establecen los distintos tipos de control interno que se refiere a: Control Interno Administrativo y Control Interno Financiero, y dentro de estos, el control previo, concurrente y posterior".

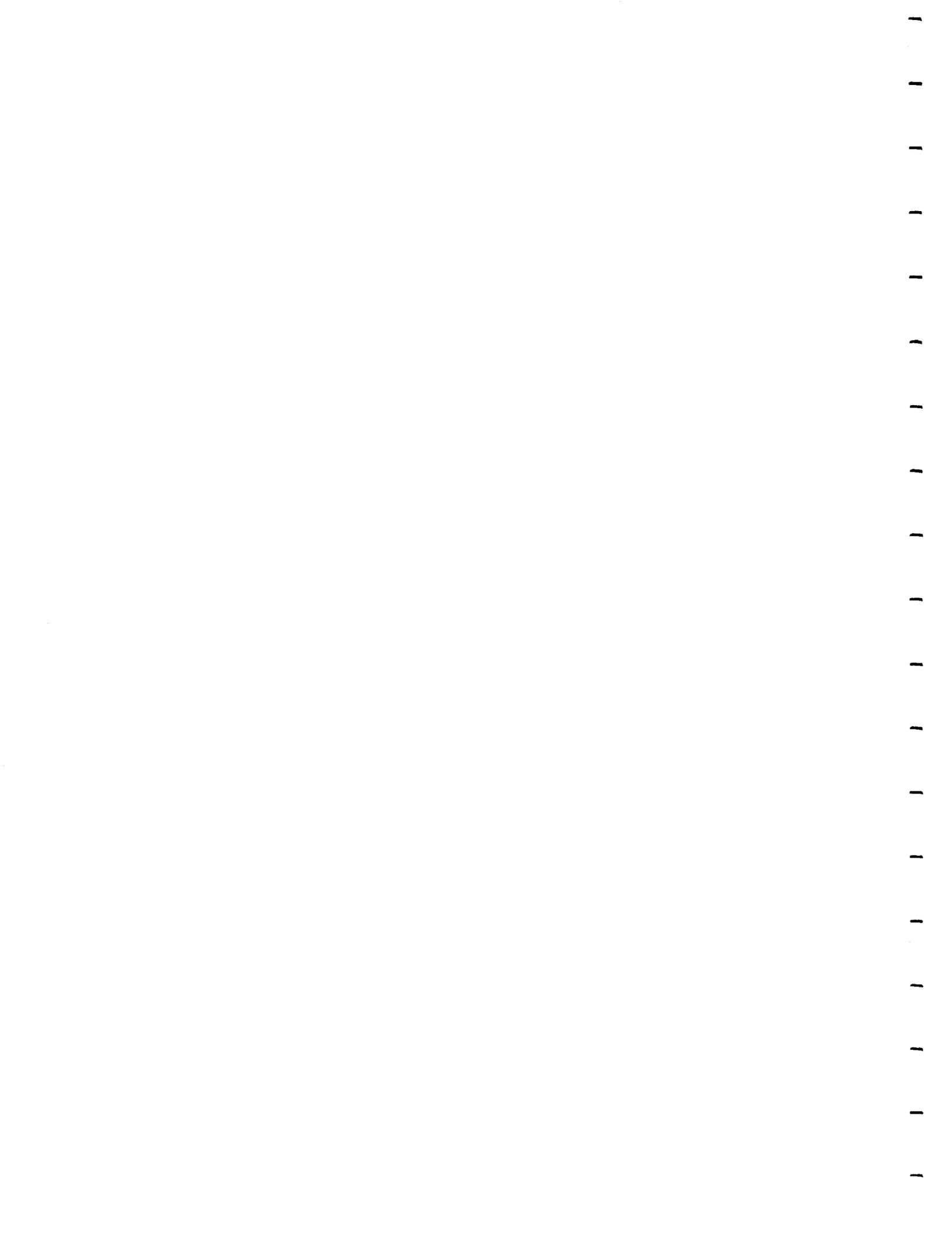
Causa

Los Administradores de la Base de Datos, no ha efectuado las gestiones para la elaboración de los procedimientos que garanticen la trazabilidad de las operaciones que realizan, así como los respaldos necesarios a través de actas administrativas para los cambios efectuados en la información almacenada, a solicitud del dueño de la información.

Efecto

Riesgo de pérdida de la trazabilidad de las operaciones que realiza el administrador de base de datos y los usuarios con la información almacenada en





la Base de Datos.

Riesgo de no tener registros de los cambios realizados a la información almacenada en la Base de Datos, por el administrador de la misma, cuando así lo requiera el dueño de la información, certificando los cambios efectuados.

Recomendación

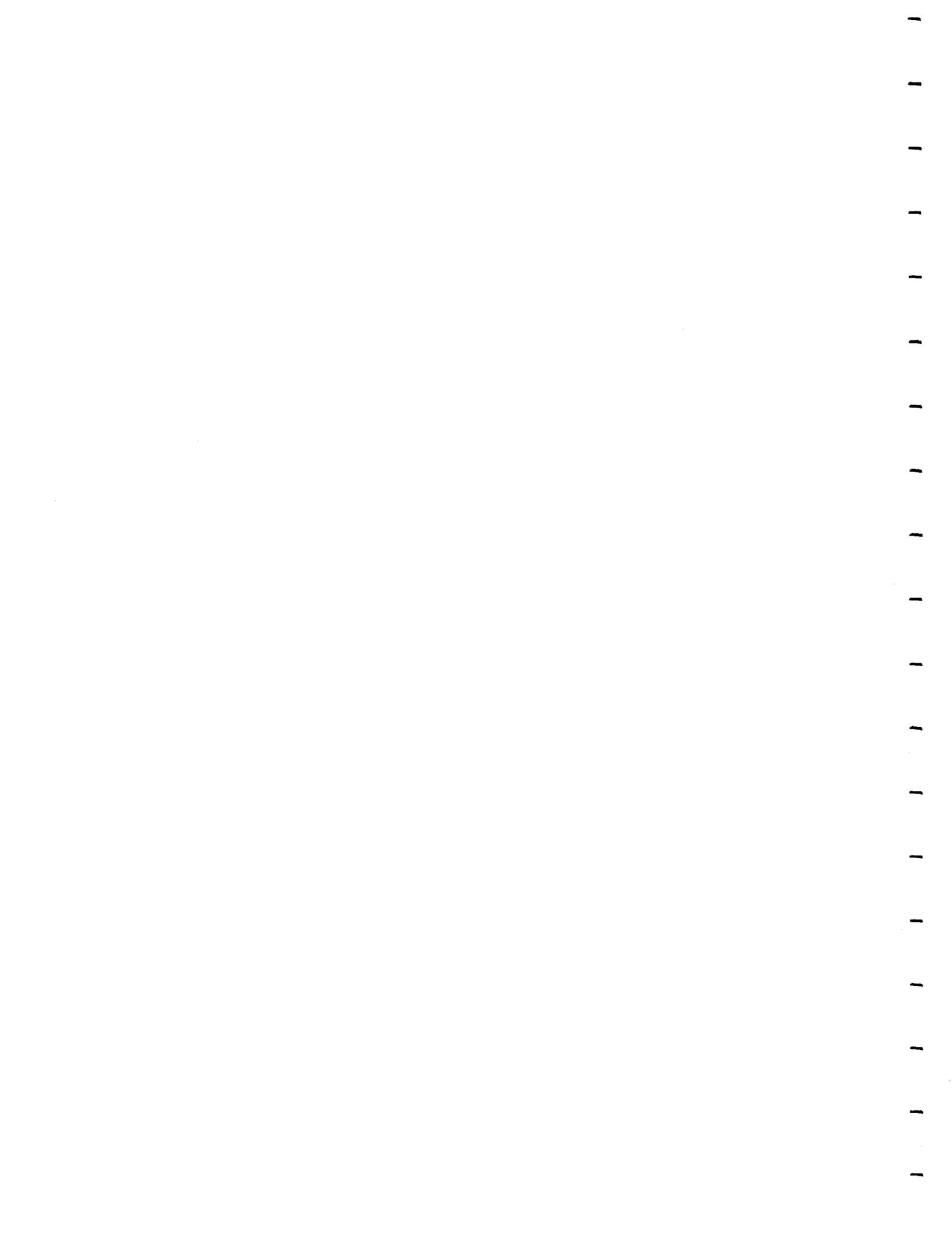
Los Administradores de la Base de Datos DBA, deben segregar las funciones dentro de la base de datos, a fin de que se creen usuarios administradores con perfiles únicamente en los esquemas de su competencia, se cree un usuario de consulta al AUDIT_TRAIL para supervisar las acciones de los usuarios, administradores y el administrador de base de datos que tenga privilegios sobre el AUDIT_TRAIL quede bajo resguardo del Director de Informática y Estadística, siendo utilizado solo en casos especiales; así mismo el Director de Informática y Estadística establezca los procedimientos adecuados para que los cambios realizados en las bases de datos a solicitud del dueño de la información, queden plasmados en actas administrativas.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Lai Yee Leung Ng, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 05 de mayo al 18 de agosto de 2015, expone lo siguiente: "En relación a lo observado que en el período auditado tiene acceso el Administrador de la Base de Datos (DBA), al módulo de Auditoría la base de datos, denominado AUDIT_TRAIL, se informa que si bien es cierto que las normas de auditoría indican sobre la segregación de funciones, lamentablemente la versión del gestor de base de datos Oracle 10gR2 (10.2.0.5) no permite desactivar o deshabilitar el rol o perfil DBA para el módulo en mención, tal cual lo confirma el informe de servicios de asesoría técnica emitido por la empresa DATUM, S.A. con fecha 09 de enero gestionado por el Ingeniero Dany Josué Minchez Monzón.

En relación a que no existe un procedimiento definido en el cual los cambios a la información de la Base de Datos solicitados por oficio por el dueño de la información, se realicen en presencia del solicitante y dicho procedimiento quede plasmado en Acta Administrativa, se informa que cualquier cambio a la información de la Base de Datos se realiza bajo el amparo de un requerimiento el cual debe estar debidamente autorizado, durante el período auditado no se realizan en presencia del usuario final debido a que el acceso a la base de datos es confidencial y que el gestor de base de datos de uso únicamente por el Departamento de Base de Datos, además en el oficio de solicitud vienen las firmas plasmadas de la máxima autoridad competente.





CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, se solicita que se tenga por desvanecido el hallazgo número cuatro (4) falta de procedimientos para el uso de bitácoras, aplicables al área técnica, derivado que en el ámbito de mi competencia se tiene acceso al módulo de Auditoría de la base de datos y actualmente no se puede desactivar o deshabilitar el rol o perfil DBA, así como los cambios a la información de la Base de Datos se realiza bajo el amparo de un requerimiento debidamente autorizado por la máxima autoridad competente.

PETICIONES:

Que se tenga por presentado en tiempo... los argumentos legales y las pruebas de descargo correspondientes;

Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos los hallazgos números 4 y 5 relacionados, formulados hacia mi persona;

Que se me notifique de la resolución de desvanecimiento de los referidos hallazgos”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Paúl Enrique Hernández Cifuentes, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 01 de enero al 17 de abril de 2015, expone lo siguiente: “En relación a que se observó que actualmente tiene acceso el Administrador de la Base de Datos (DBA), al módulo de Auditoría de la base de datos, denominado AUDIT_TRAIL, se informa que compete al administrador de base de datos (DBA) supervisar la administración de la base de datos de la Institución y adoptar medidas tendentes a garantizar el correcto funcionamiento e integridad de esta, realizar estudios y proponer medidas para la optimización de la base de datos, dirigir o llevar a cabo todas las actividades relacionadas con el mantenimiento, así como correcto funcionamiento, implementando las normas y políticas necesarias para el resguardo de la información en los medios de almacenamiento y mantener un monitoreo constante; teniendo en cuenta las funciones del Administrador de la Base de Datos no se debe considerar como un hallazgo el que se tenga acceso al módulo de Auditoría, según las funciones que como Administrador de base de datos son atribuidas.

Como un valor agregado el Administrador de la Base de Datos (DBA) cuenta con un informe de servicios de asesoría técnica de fecha 07 de enero del año en curso de la Empresa: DATUM, S.A. en donde se indica que en la versión 10gR2 (10.2.0.5), no es posible desactivar o deshabilitar el rol o perfil DBA, versión que se encontraba en funcionamiento en el periodo auditado.

En relación a que no existe un procedimiento definido en el cual los cambios a la información de la Base de Datos solicitados por oficio por el dueño de la





información, se realicen en presencia del solicitante y dicho procedimiento quede plasmado en Acta Administrativa, se informa que cualquier cambio a la información de la Base de Datos se realiza bajo el amparo de un requerimiento (Oficio) el cual debe estar debidamente autorizado y posteriormente analizado para su ejecución; durante el periodo auditado no se realizan cambios en presencia del usuario final debido a que el acceso a la base de datos es confidencial y de uso exclusivo por personal calificado del Departamento de Base de Datos, además en el oficio de solicitud vienen las firmas plasmadas de la máxima autoridad competente.

CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, se solicita que se tenga por desvanecido el hallazgo número cuatro (4) falta de procedimientos para el uso de bitácoras, aplicables al área técnica, derivado que en el ámbito de la competencia del Administrador de Base de Datos se tiene acceso al módulo de Auditoría de la base de datos y actualmente no se puede desactivar o deshabilitar el rol o perfil DBA, así como los cambios a la información de la Base de Datos se realiza bajo el amparo de un requerimiento (oficio) debidamente autorizado por la máxima autoridad competente.

PETICIONES:

Que se tenga por presentado en tiempo el presente memorial que contiene los argumentos legales y las pruebas de descargo correspondientes; así como las pruebas presentadas por el Administrador de la Base de Datos del Registro Nacional de las Personas – RENAP –, dado que ya no laboro para la institución mencionada y no cuento con acceso a dicha información.
Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos los hallazgos números 4 y 5 relacionados, formulados hacia mi persona;
Que se me notifique de la resolución de desvanecimiento de los referidos hallazgos”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Dany Josué Míncuez Monzón, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 01 de julio al 31 de octubre 2016, expone lo siguiente: “En relación a que se observó que actualmente tiene acceso el Administrador de la Base de Datos (DBA), al módulo de Auditoría de la base de datos, denominado AUDIT_TRAIL, informo que compete al administrador de la base de datos (DBA) supervisar la administración de la base de datos de la Institución y adoptar medidas tendentes a garantizar el correcto funcionamiento e integridad de esta, realizar estudios y proponer medidas para la optimización de la base de datos, dirigir o llevar a cabo todas las actividades relacionadas con el mantenimiento, así como correcto funcionamiento, implementando las normas y políticas necesarias para el resguardo de la información en los medios de almacenamiento y mantener





un monitoreo constante; teniendo en cuenta las funciones del Administrador de la Base de Datos no se debe considerar como un hallazgo el que se tenga acceso al módulo de Auditoría, según las funciones que como Administrador de base de datos me son atribuidas.

Como un valor agregado se cuenta con un informe de servicios de asesoría Técnica de fecha 09 de enero del año en curso de la Empresa: DATUM, S.A. en donde se indica que en la versión actual 10Gr2 (10.2.0.5), no es posible desactivar o deshabilitar el rol o perfil DBA.

En relación a que no existe un procedimiento definido en el cual los cambios a la información de la Base de Datos solicitados por oficio por el dueño de la información, se realicen en presencia del solicitante y dicho procedimiento quede plasmado en Acta Administrativa, informo que cualquier cambio a la información de la Base de Datos se realiza bajo el amparo de un requerimiento el cual debe estar debidamente autorizado, actualmente no se realizan en presencia del usuario final debido a que el acceso a la base de datos es confidencial y de uso únicamente por el Departamento de Base de Datos, además en el oficio ya vienen las firmas plasmadas de la máxima autoridad competente.

CONCLUSIÓN:

En virtud de los preceptos legales referidos y la exposición de motivos indicados, solicito que se tenga por desvanecido el hallazgo número cuatro (4) falta de procedimientos para el uso de bitácoras, aplicables al área técnica, derivado a que en el ámbito de mi competencia se tiene acceso al módulo de Auditoría de la base de datos y actualmente no se puede desactivar o deshabilitar el rol o perfil DBA, así como los cambios a la información de la Base de Datos se realiza bajo el amparo de un requerimiento debidamente autorizado por la máxima autoridad competente.

PETICIONES

Que se tenga por presentado en tiempo los argumentos legales y las pruebas de descargo correspondientes;

Que una vez evaluadas las pruebas de descargo se tenga por desvanecido el hallazgo 5 relacionado, formulado hacia mi persona;

Que se me notifique de la resolución de desvanecimiento del referido hallazgo".

Comentario de la Auditoría

Se confirma el presente hallazgo para el señor Paul Enrique Hernández Cifuentes, quién fungió como Jefe de Base de Datos durante el período del 01 de enero de 2015 al 17 de abril de 2015; para la señora Lai Yee Leung Ng, quién fungió como Jefe de Base de Datos durante el período del 05 de mayo al 18 de agosto de 2015



y para el señor Dany Josué Minchez Monzon, quién fungió como Jefe de Base de Datos durante el período del 01 de julio de 2015 al 31 de octubre de 2016 ya que luego de analizar las pruebas de descargo presentadas se determinó que aunque no es posible desactivar o deshabilitar en el rol o perfil de Administrador de Base de Datos (DBA) los privilegios sobre el AUDIT_TRAIL, se pueden crear usuarios administradores con perfiles sobre las instancias y bases de datos que sean de su competencia y así mejorar la segregación de funciones dentro de la base de datos. Adicionalmente no se han efectuado las gestiones necesarias para que los cambios realizados en las bases de datos a solicitud del dueño de la información consten en actas administrativas.

Este hallazgo fue notificado con el número 4 y corresponde en el presente hallazgo al número 2.

Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
JEFE DE BASE DE DATOS	PAUL ENRIQUE HERNANDEZ CIFUENTES	4,500.00
JEFE DE BASE DE DATOS	LAI YEE LEUNG NG	4,500.00
JEFE DE BASE DE DATOS	DANY JOSUE MINCHEZ MONZON	4,500.00
Total		Q. 13,500.00

Hallazgo No. 3

Desactualización de los Parches en la base de Datos

Condición

En el Registro Nacional de las Personas -RENAP-, se carece de procedimientos y de una plataforma en donde se puedan efectuar los escenarios de prueba para la actualización de Parches, los cuales sirven para prevenir cualquier vulnerabilidad que afecte al sistema gestor de la base de datos.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.6, Tipos de Controles, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, establecer e implementar con claridad los diferentes tipos de control que se relacionan con los sistemas administrativos y financieros. En el Marco Conceptual de Control Interno Gubernamental, se establecen los distintos tipos de control interno que se refiere a: Control Interno Administrativo y Control Interno Financiero, y dentro de estos, el control previo, concurrente y posterior".



Causa

Los Administradores de la Base de Datos -DBA-, no han efectuado las gestiones necesarias para crear una plataforma y un ambiente en el cual se puedan realizar las pruebas requeridas para llevar a cabo las actualizaciones de parches al sistema gestor de la Base de datos.

Efecto

Riesgo de pérdida de información crítica de la entidad, por la falta de actualización de parches al sistema gestor de la base de datos, lo que provocaría falta de credibilidad en los servicios que presta el Registro Nacional de las Personas.

Recomendación

El Director de Informática y Estadística, debe girar instrucciones a los Administradores de la Base de Datos, para que se elabore el procedimiento que incluya un ambiente de pruebas para la realización de las actualizaciones de parches que requiera el sistema gestor de Base de Datos, como una medida preventiva para mitigar los riesgos en el sistema que podrían surgir por no realizarlas actualizaciones.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Lai Yee Leung Ng, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 05 de mayo al 18 de agosto de 2015, expone lo siguiente: "...se informa que con fecha 15 de abril del año 2015 se emitió oficio REF.: DI-DBA-0013-2015 dirigido al Director de Informática y Estadística, en donde el Administrador de base de Datos solicita Hardware para poder implementar una base de datos de prueba.

CONCLUSIÓN:

Por lo anterior expuesto, se solicita que se tenga por desvanecido el hallazgo número cinco (5) de control interno del área técnica, derivado que en su momento el Administrador de Base de Datos hizo el requerimiento al Director de Informática y Estadística lo necesario para tener una instancia de pruebas tal cual lo recomienda los auditores de Contraloría General de Cuentas.

PETICIONES:

Que se tenga por presentado en tiempo los argumentos legales y las pruebas de descargo correspondientes;
Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos los hallazgos números 4 y 5 relacionados y formulados hacia mi persona;
Que se me notifique de la resolución de desvanecimiento de los referidos hallazgos".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Paúl Enrique





Hernández Cifuentes, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 01 de enero al 17 de abril de 2015, expone lo siguiente: "En relación a lo anterior, se informa que con fecha 15 de abril del año 2015 el Administrador de Base de Datos emitió oficio REF.: DI-DBA-0013-2015 dirigido al Director de Informática y Estadística, en donde se solicita Hardware para poder implementar una base de datos de prueba.

CONCLUSIÓN:

Derivado de lo expuesto con anterioridad, se solicita que se tenga por desvanecido el hallazgo número cinco (5) de control interno del área técnica, derivado que en su momento le fue requerido al Director de Informática y Estadística lo necesario para tener una instancia de pruebas y desconociendo la acción tomada en relación a dicha solicitud dado el período de vigencia de mi contrato laboral, el cual concluyó el 17 de abril de 2015.

PETICIONES:

Que se tenga por presentado en tiempo el presente memorial que contiene los argumentos legales y las pruebas de descargo correspondientes; así como las pruebas presentadas por el Administrador de la Base de Datos del Registro Nacional de las Personas – RENAP –, dado que ya no laboro para la institución mencionada y no cuento con acceso a dicha información. Que una vez evaluadas las pruebas de descargo se tengan por desvanecidos los hallazgos números 4 y 5 relacionados, formulados hacia mi persona; Que se me notifique de la resolución de desvanecimiento de los referidos hallazgos".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Dany Josué Míncuez Monzón, Jefe de Base de Datos del Registro Nacional de las Personas, durante el período del 01 de julio de 2015 al 31 de octubre de 2016, expone lo siguiente: "En relación a lo anterior se informa que el 16 de abril del año 2015 mediante oficio REF.: DI-DBA-0013-2015 dirigido al Director de Informática y Estadística, se solicitó Hardware para poder implementar una base de datos de prueba".

CONCLUSIÓN:

Derivado de lo expuesto con anterioridad solicito que se tenga por desvanecido el hallazgo número cinco (5) de control interno del área técnica, derivado a que en su momento le fue requerido al Director de Informática y Estadística lo necesario para tener una instancia de pruebas.

PETICIONES:

Que se tenga por presentado en tiempo los argumentos legales y las pruebas de descargo correspondientes;
Que una vez evaluadas las pruebas de descargo se tengan por desvanecido el





hallazgo número 5 relacionado, formulado hacia mi persona.
Que se me notifique de la resolución de desvanecimiento del referido hallazgo”.

Comentario de la Auditoría

Se confirma el presente hallazgo para el señor Paul Enrique Hernández Cifuentes, quién fungió como Jefe de Base de Datos durante el período del 01 de enero de 2015 al 17 de abril de 2015; para la señora Lai Yee Leung Ng, quién fungió como Jefe de Base de Datos durante el período del 05 de mayo al 18 de agosto de 2015 y para el señor Dany Josué Minchez Monzon, quién fungió como Jefe de Base de Datos durante el período del 01 de julio de 2015 al 31 de octubre de 2016 ya que luego de analizar las pruebas de descargo presentadas se determinó que de acuerdo al oficio Ref.: DI-DBA-0013-2015 se realizó solicitud de un ambiente de pruebas, adicionalmente este fue girado por el Administrador de Base de Datos sin contar con el visto bueno del Jefe de Base de Datos, en tal sentido no se evidencia ningún tipo seguimiento a lo solicitado en dicho oficio.

Este hallazgo fue notificado con el número 5 y corresponde en el presente informe al número 3.

Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
JEFE DE BASE DE DATOS	PAUL ENRIQUE HERNANDEZ CIFUENTES	4,500.00
JEFE DE BASE DE DATOS	LAI YEE LEUNG NG	4,500.00
JEFE DE BASE DE DATOS	DANY JOSUE MINCHEZ MONZON	4,500.00
Total		Q. 13,500.00

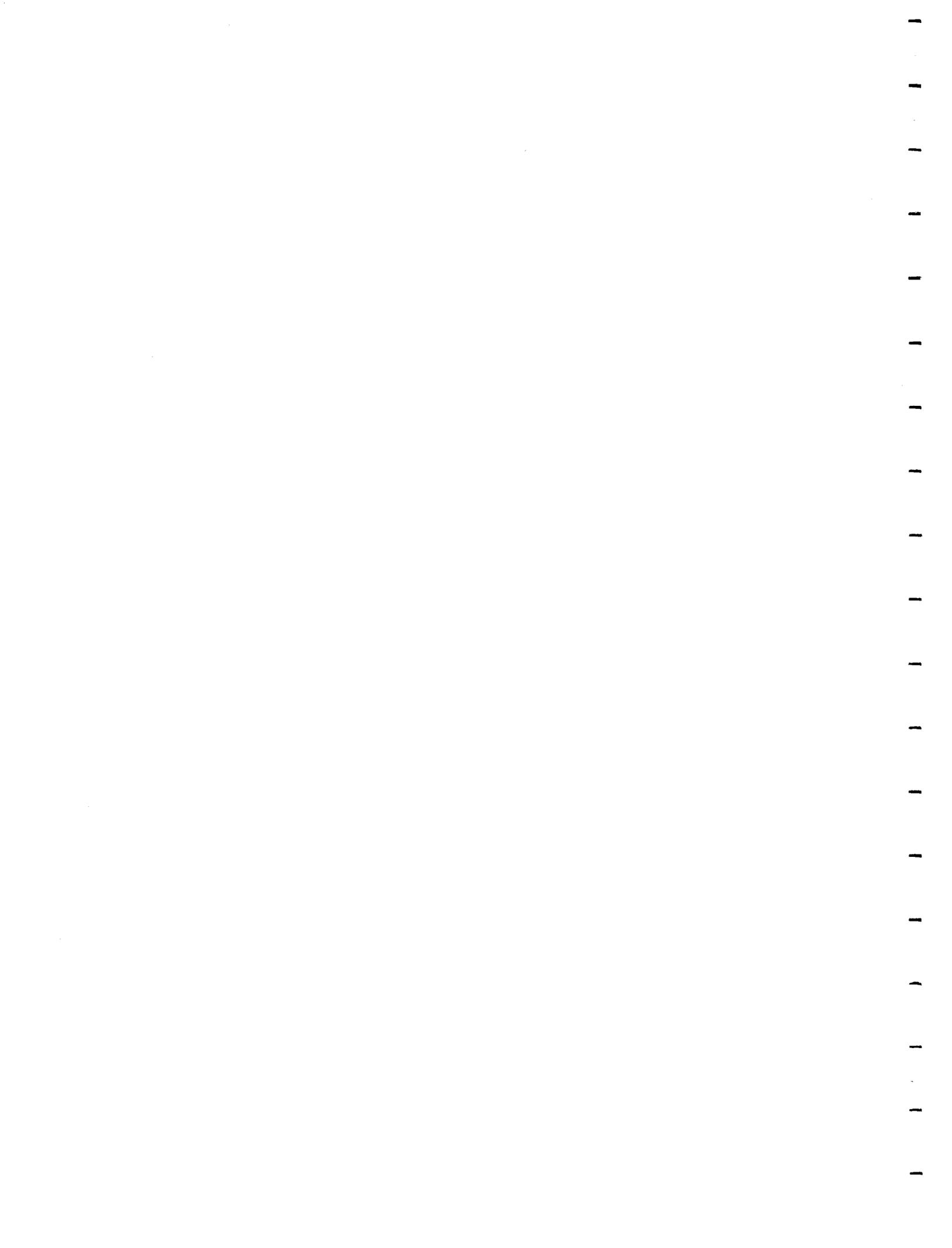
Hallazgo No. 4

Falta de un Plan de Continuidad del Negocio -BCP-

Condición

En el Departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, se determinó al efectuar la auditoría a sistemas informáticos que no cuentan con un Plan de Continuidad del Negocio, (Business Continuity Planning -BCP-), a nivel de tecnología de la información, aprobado por la Dirección Ejecutiva en donde se detalle las actividades en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección Informática y Estadística.





Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.2 Estructura de Control Interno, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, diseñar e implantar una estructura efectiva de control interno, que promueva un ambiente óptimo de trabajo para alcanzar los objetivos institucionales.

Una efectiva estructura de control interno debe incluir criterios específicos relacionados con: a) controles generales; b) controles específicos; c) controles preventivos; d) controles de detección; e) controles prácticos; f) controles funcionales; g) controles de legalidad; y, h) controles de oportunidad, aplicados en cada etapa del proceso administrativo, de tal manera que se alcance la simplificación administrativa y operativa, eliminando o agregando controles, sin que se lesione la calidad del servicio."

Causa

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental; numeral 1.2 Estructura de Control Interno, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, diseñar e implantar una estructura efectiva de control interno, que promueva un ambiente óptimo de trabajo para alcanzar los objetivos institucionales.

Una efectiva estructura de control interno debe incluir criterios específicos relacionados con: a) controles generales; b) controles específicos; c) controles preventivos; d) controles de detección; e) controles prácticos; f) controles funcionales; g) controles de legalidad; y, h) controles de oportunidad, aplicados en cada etapa del proceso administrativo, de tal manera que se alcance la simplificación administrativa y operativa, eliminando o agregando controles, sin que se lesione la calidad del servicio."

Efecto

Riesgo de pérdida de la continuidad de los servicios críticos a nivel tecnológico, al no contar con procesos claros y responsables definidos a fin de reanudar los servicios críticos, lo que provocaría la falta de servicio en los sistemas principales del registro, afectando la imagen y credibilidad del Registro Nacional de las Personas.

Recomendación

El Directorio del Registro Nacional de las Personas debe girar instrucciones al Director Ejecutivo, Director de Informática y Estadística, Subdirector de Sistemas y





Estadística y Subdirector de Servicios Críticos, para que se elabore un plan de continuidad del negocio, en donde se establezcan los procedimientos internos a realizar y se especifique a los responsables en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección Informática y Estadística.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Eduardo Salvador Navarro Molina, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período del 16 de mayo al 21 de septiembre de 2015, expone lo siguiente: "...me permito manifestar lo siguiente:

BASE LEGAL:

Acuerdo de Dirección Ejecutiva del Registro Nacional de las Personas -RENAP- número DE 147-2016, en el cual se aprueba el Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

ACCIONES EFECTUADAS:

Se realizaron varias reuniones de trabajo para dar seguimiento al Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP, durante el periodo que desempeñe el puesto de Subdirector de Servicios Críticos. Que se cuenta con un Plan de contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

En la fecha que desempeñe el cargo de Subdirector de Servicios Críticos, se desarrolló el Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

DOCUMENTOS DE PRUEBA:

Acuerdo de Dirección Ejecutiva del Registro Nacional de las Personas -RENAP- número DE 147-2016, en el cual se aprueba el Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

Plan de Contingencia para la Continuidad de Operaciones Informáticas en el RENAP.

Acta número 26-2016 de la Sub-Dirección de Recursos Humanos, Dirección Administrativa del Registro Nacional de las Personas Renap, de toma de posesión del cargo de Subdirector de Servicios Críticos de la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- del 16 de mayo del año 2016.

Solicitud:

Que se valoren los documentos presentados como respaldo utilizado de base para





soportar las pruebas de descargado.

Luego de su evaluación y análisis, procedan a darlos por aceptados y procedan a DESVANECER LOS POSIBLES HALLAZGOS DESCRITOS.

Se haga de mi conocimiento, la resolución final sobre el desvanecimiento del posible hallazgo comentado en esta diligencia, o se me indique las razones que le asisten a esa Comisión de Auditoría Gubernamental, para confirmar los mismos”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Rudy Leonel Gallardo Rosales, Director Ejecutivo del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 01 de junio de 2016, expone lo siguiente: “No es cierto lo indicado por los señores auditores. En mi calidad de Director Ejecutivo del RENAP sí elaboré una Política y el Alcance del Sistema de Gestión de Continuidad del Negocio que es la primera fase para la creación de dicho plan. Estos dos documentos fueron aprobados por mi persona el 29 de abril de 2016. De tal manera que si impulsé la formulación del Plan de Continuidad de Negocios, sin embargo, debe indicarse que se trata de un proceso complejo en virtud de la magnitud de la institución, y su inicio es precisamente la definición y aprobación de la Política y el Alcance. Posteriormente, la Dirección de Gestión y Control Interno del RENAP siguió trabajando en el documento, el cual terminó a finales de Julio de 2016 y se le trasladó a la entonces Directora Ejecutiva, Ingeniera Brenda Amarilis Gramajo para su aprobación posterior, ignorando si se continuó con el trabajo que yo había iniciado como Director Ejecutivo, puesto que como ya he indicado, fui detenido el 2 de junio de 2016, situación que persiste hasta el momento, pero puede determinarse claramente, que no tengo responsabilidad en el supuesto hallazgo a ese respecto. Cabe agregar que el 26 de julio de 2016, no obstante no estar yo en funciones de Dirección Ejecutiva, se elaboró el Plan de Continuidad del Negocio del RENAP.

PRUEBAS DE DESCARGO EN CUANTO A ESTE HALLAZGO:

Copia del oficio Ref. DE-1287-2016 de fecha 29 de abril de 2016 que remite el Alcance del Sistema de Gestión de Continuidad del Negocio a la Dirección de Gestión y Control Interno;

Copia del oficio Ref. DE-1286-2016 de fecha 29 de abril de 2016 que remite la Política de Continuidad del Negocio a la Dirección de Gestión y Control Interno;

Copia del Plan de Continuidad del Negocio del RENAP de fecha 26 de julio de 2016.

PETICIONES:

Que se tenga por presentados de mi parte los argumentos legales y pruebas de descargo correspondientes;

Que se proceda a evaluar las argumentaciones vertidas de mi parte.

Que una vez evaluadas las argumentaciones y pruebas de descargo, se tenga por DESVANECIDOS los hallazgos relacionados, por las razones ya argumentadas de



mi parte.

Que se sirvan notificarme el desvanecimiento de los referidos hallazgos”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Héctor Iván García Solórzano, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período del 16 de mayo al 21 de septiembre de 2016, expone lo siguiente: “Yo, Héctor Iván García Solórzano, identificándome con DPI 2220 38918 0101 respetuosamente comparezco ante esta entidad contralora a evacuar la audiencia conferida y en consecuencia; hago constar que estuve en el cargo como subdirector de Servicios Críticos del 01 de julio de 2015 al 31 de marzo del 2016, presentando mi renuncia al puesto a la Dirección Ejecutiva el 28 de marzo de 2016, y se acepta mi renuncia el 31 de marzo de 2016 mediante oficio DA-SHR-dg-576-2016, haciendo constar que durante 8 meses de ocupar el puesto fue muy corto para poder evaluar y ejercer control en la subdirección de Servicios Críticos.

RAZONAMIENTO:

La dirección de informático si cuenta con el “Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Renap”, identificado bajo el código -Plan 032016- versión 1, autorizado por la jefatura de gestión de la calidad de la dirección de control y gestión interno, y firmado por la dirección ejecutiva.

CONCLUSIÓN:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número seis (6), respecto a que no se cuente con el “Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Renap”, derivado a que si se tiene dicho plan”.

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Brenda Amarilis Gramajo González, Director Ejecutivo del Registro Nacional de las Personas, durante el período del 08 de octubre de 2015 al 31 de octubre de 2016, expone lo siguiente: “El Reglamento de Organización y Funciones del RENAP, establece lo siguiente:

“Artículo 46 Dirección de Informática y Estadística. Es la dependencia encargada de dirigir las actividades relacionadas con el almacenamiento y procesamiento de los datos que se originen en el Registro Central de las Personas, en relación a su estado civil, capacidad civil y demás datos de identificación...”, “...Para la protección de la base de datos, ésta dependencia tendrá a su cargo la custodia y elaboración de los respaldos electrónicos, vigilando porque de los mismos se efectúe un respaldo en un sitio remoto y éste sea realizado en forma simultánea y



su procesamiento en el sitio central del RENAP, velando por que se cumplan las normas y mejores prácticas en materia de tecnología que garanticen la absoluta seguridad.

Asimismo las literales siguientes establecen:

“...d) Definir previo análisis, los lineamientos y requerimientos técnicos para la adquisición de tecnologías, sistemas de información y comunicación que servirán para el desarrollo tecnológico de la Institución...”.

“...e) Planificar, dirigir y coordinar el desarrollo, instalación y administración de los sistemas y equipos informáticos y de comunicaciones...”.

“...h) Resguardar la información en la base de datos del RENAP, de acuerdo a la política de seguridad de la información establecida por la institución, y tener un respaldo (backup) de dicha información...”.

Al respecto, es importante se tome en consideración que según la norma legal citada, se establece que la Dirección de Informática es la dependencia que tendrá a su cargo la custodia y elaboración de los respaldos electrónicos, vigilando porque de los mismos se efectúen un respaldo en un sitio remoto y éste sea realizado en forma simultánea y su procesamiento en el sitio central del RENAP, velando por que se cumplan las normas y mejores prácticas en materia de tecnología que garanticen la absoluta seguridad; asimismo es responsable de Resguardar la información en la base de datos del RENAP, de acuerdo a la política de seguridad de la información establecida por la institución, y tener un respaldo (backup) de dicha información...”.

Con relación a que no se cuenta con un Plan de Continuidad de Negocio (Business Continuity Planning -BCP-), a nivel de tecnología de información, es importante hacer del conocimiento de la Comisión de Auditoría Gubernamental, lo siguiente:

Por medio de oficio Ref.DE-1286-2016 de fecha 29 de abril de 2016, el Despacho de Dirección Ejecutiva del RENAP, remitió a la Dirección de Gestión y Control Interno, el documento que contiene la Política de Continuidad del Negocio, Norma UNE-EN-ISO-2231-2015 (Versión 1), para su debida divulgación e implementación.

Por medio de oficio Ref.DE-1289-2016 de fecha 29 de abril de 2016, el Despacho de Dirección Ejecutiva del RENAP, remitió a la Dirección de Gestión y Control Interno el documento original que contiene la Política de Seguridad de la Información. (versión 2), para su divulgación e implementación.

Plan de Contingencia para la Continuidad de Operaciones Informáticas en el





RENAP, aprobado en el año 2016, bajo el código Plan 03-2016, versión 01.

En ese sentido, la Institución ha tomado las acciones necesarias que garantizan la continuidad de los servicios críticos a nivel tecnológico, contando la Dirección de Informática y Estadística, con las herramientas que definen procesos claros y responsables que permiten garantizar la continuidad de los servicios críticos ante eventos que pudieren suscitarse en un momento dado, por lo que se desvirtúan los criterios vertidos por la Comisión de Auditoría Gubernamental”.

Mediante oficio s/n y sin fecha, el señor Carlos Alberto Quintana Galindo, Director de Informática y Estadística del Registro Nacional de las Personas, durante el período del 01 de julio de 2014 al 01 de agosto de 2016, indica lo siguiente: “La dirección de informático si cuenta con el “Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Renap”, identificado bajo el código -Plan 032016- versión 1, autorizado por la jefatura de gestión de la calidad de la dirección de control y gestión interno, y firmado por la dirección ejecutiva. Se adjunta la autorización de dicha política, misma que se encuentra en la dirección de informática.

PETICION:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número seis (6), respecto a que no se cuente con el “Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Renap”, derivado a que si se tiene dicho plan”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Dante Antonio Ávalos Aguilar, Director de Gestión y Control Interno del Registro Nacional de las Personas, durante el período del 01 de enero al 25 de octubre de 2016, expone lo siguiente: “De acuerdo con la condición y la causa expresada en el Hallazgo No. 6 “Falta un Plan de Continuidad del Negocio -BCP-, se determinó que en el Departamento de Análisis de Sistemas de Información del RENAP, no cuentan con un Plan de Continuidad del Negocio (Business Continuity Plan -BCP-), a nivel de tecnología de la información, aprobado por la Dirección Ejecutiva, en donde se detalle las actividades en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección de Informática y Estadística. La causa es porque el Director Ejecutivo del RENAP, el Director de Informática y Estadística, el Subdirector de Sistemas y Estadística y el Subdirector de Servicios Críticos, no han implementado un plan de continuidad que permita restituir rápidamente los servicios de la organización, ante eventos que puedan presentarse en los servicios ya sea de forma parcial o total.

Como puede leerse en el hallazgo, no se encuentra como una de las causas que el Director de Gestión y Control Interno no haya implementado el Plan de



Continuidad de Negocios. Esto se debe a que la Dirección de Gestión y Control Interno no tiene dentro de sus funciones la implementación de dicha medida, mientras que sí es responsabilidad del Director, Subdirectores y Jefes de Departamento de la Dirección de Informática y Estadística. Estas funciones pueden encontrarse en el Decreto No. 90-2005, emitido por el Congreso de la República, en el Capítulo VII, en donde se establecen las Direcciones Administrativas y sus funciones correspondientes.

El artículo 42, describe la Dirección de Informática y Estadística. Como puede observarse en dicho artículo, descrito a continuación, la Dirección de Informática y Estadística es el ente encargado de dirigir las actividades relacionadas con el almacenamiento y procesamiento de los datos que se originen en el Registro Central. Además, tendrá a su cargo la custodia y elaboración de los respaldos electrónicos, vigilando porque de los mismos se efectúe también un respaldo en un sitio remoto y éste sea realizado en forma simultánea con el ingreso de los datos y su procesamiento en el sitio central del RENAP, velando porque se cumplan las normas y mejores prácticas en materia tecnológica que garanticen su absoluta seguridad.

Por otra parte, en el artículo 46, se presentan las funciones de la Dirección de Gestión y Control Interno, y se puede verificar que en sus funciones está la formulación de planes y programas institucionales, por lo que como se puede observar no implementa o ejecuta, sólo formula.

CAPÍTULO VII

DIRECCIONES ADMINISTRATIVAS

Artículo 42. Dirección de Informática y Estadística. La Dirección de Informática y Estadística es el ente encargado de dirigir las actividades relacionadas con el almacenamiento y procesamiento de los datos que se originen en el Registro Central de las Personas, en relación a su estado civil, capacidad civil y demás datos de identificación. Formula los planes y programas de la Institución en la materia de su competencia, informa sobre el cumplimiento de las metas institucionales programadas y elabora las estadísticas pertinentes.

Para la protección de la base de datos, esta dependencia tendrá a su cargo la custodia y elaboración de los respaldos electrónicos, vigilando porque de los mismos se efectúe también un respaldo en un sitio remoto y éste sea realizado en forma simultánea con el ingreso de los datos y su procesamiento en el sitio central del RENAP, velando porque se cumplan las normas y mejores prácticas en materia tecnológica que garanticen su absoluta seguridad. Se regirá por el reglamento respectivo.

Artículo 46. Dirección de Gestión y Control Interno. La Dirección de Gestión y Control Interno es la dependencia encargada de la formulación de planes y





programas institucionales, de fiscalizar la gestión administrativa de los funcionarios del RENAP y vigilar el desempeño administrativo, para asegurar el estricto cumplimiento de la normatividad que lo rige. Se regulará además por el reglamento respectivo.

En conclusión, derivado de las funciones establecidas en el decreto 90-2005, se puede establecer claramente que la responsabilidad de implementar el Plan de Continuidad del Negocio corresponde a la Dirección de Informática y Estadística y no a la Dirección de Gestión y Control Interno. En este caso, es responsabilidad de la Dirección de Informática y Estadística la implementación del Plan de Continuidad de Negocios, puesto que corresponde a funciones a cargo de la Dirección de Informática y Estadística.

Por otra parte, tomando en cuenta las Normas Generales de Control Interno, Norma 1.10, quiero referirme al Manual de Normas y Procedimientos establecido para el proceso de elaboración y aprobación de los Documentos Técnico Administrativos, identificado como DTA-MNP- 01- 2015, aprobado en fecha 19 de marzo de 2015 (Anexo 3). Del referido Manual, es importante en principio mencionar que fue elaborado tomando como base las Normas Generales de Control Interno Gubernamentales y al respecto, me permito citar algunas de las Normas para el diseño, elaboración y aprobación de documentos técnico administrativo.

En la norma 6.2, se establece que la máxima autoridad de cada dependencia, será responsable de que existan documentos técnico-administrativos que regulen las diferentes actividades que realizan, así como de promover y apoyar la elaboración de los mismos.

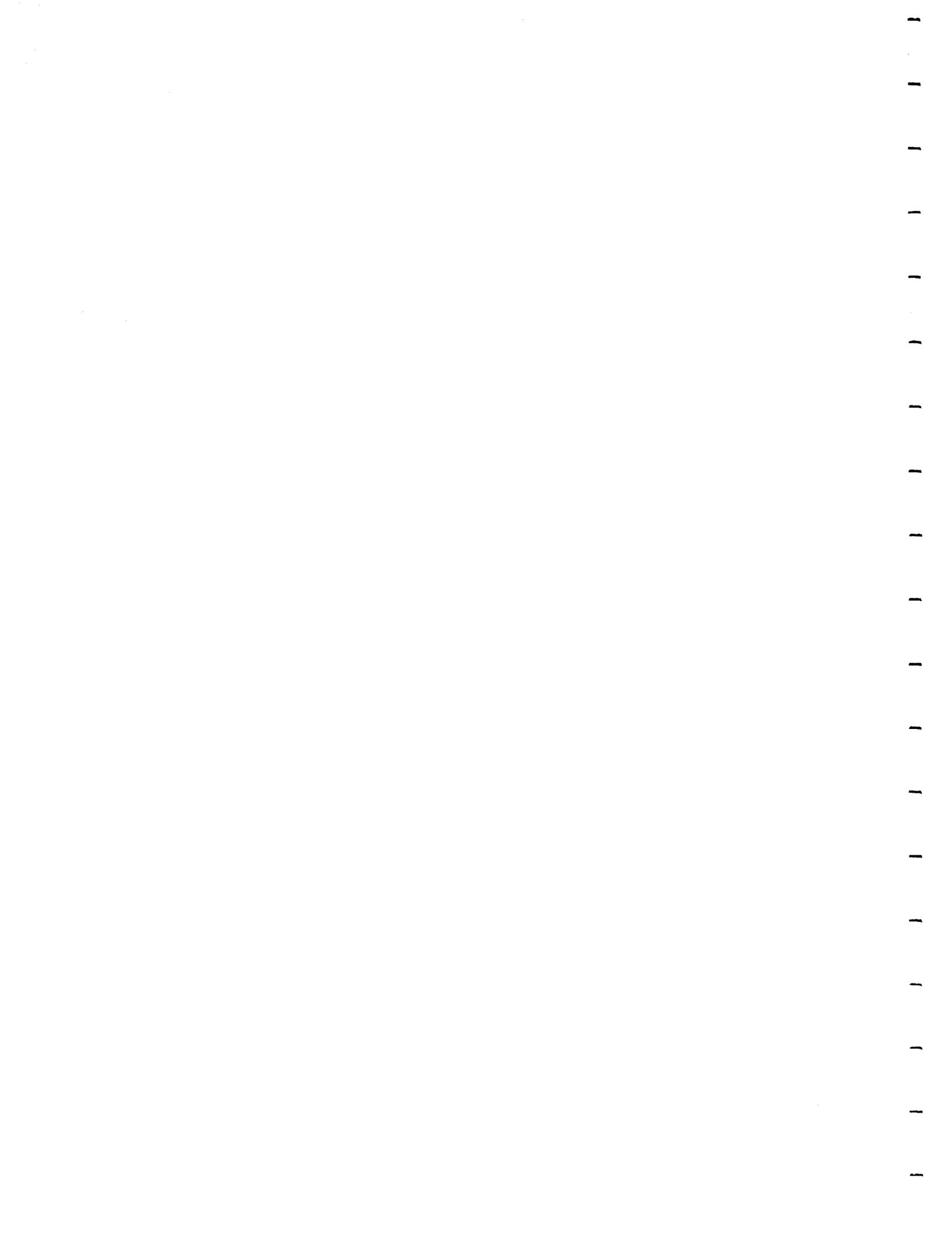
La norma 6.3, establece que el documento técnico-administrativo se elaborará con base a la información que proporcione el solicitante y/o el enlace designado.

Por otra parte, la norma 6.4 indica que la máxima autoridad de cada dependencia, será responsable de verificar y validar la información contenida en el documento técnico administrativo que regule su actuar.

La norma 6.5 establece que la máxima autoridad de cada dependencia, será responsable de actualizar los documentos técnico-administrativos para mantener su vigencia, así como solicitar la actualización cuando corresponda.

La norma 6.6 refiere que la máxima autoridad de cada dependencia, será responsable de promover una adecuada divulgación y capacitación al personal, respecto a los documentos técnico administrativos aprobados, para su adecuada implementación y aplicación.





En este sentido, después de haber citado las normas anteriores, quiero referirme a que la Dirección de Informática y Estadística del RENAP es la dependencia rectora en materia de almacenamiento y procesamiento de los datos, custodia y elaboración de respaldos electrónicos, así como cumplimiento de normas y mejores prácticas en materia tecnológica que garanticen su seguridad, y dentro de estos procesos se encuentra la implementación del Plan de Continuidad de Negocios, que garantice la continuidad de los servicios críticos ante cualquier eventualidad o contingencia.

Las máximas autoridades de la Dirección de Informática y Estadística son el Director y los Subdirectores, autoridades mencionadas en el Hallazgo No. 6 "Falta de un Plan de Continuidad del Negocio -BCP-", por lo que son quienes deben velar que los procesos se encuentren debidamente documentados por instrumentos técnicos, en este caso, por el Plan de Continuidad de Negocios -BCP-.

En conclusión, las normas anteriores claramente indican que la máxima autoridad de cada dependencia, será responsable de que existan documentos técnico-administrativos que regulen las diferentes actividades que realizan, así como de promover y apoyar la elaboración de los mismos. En este caso, es responsabilidad de la Dirección de Informática y Estadística la implementación del Plan de Continuidad de Negocios, puesto que corresponde a funciones a cargo de la Dirección de Informática y Estadística.

Finalmente, es preciso mencionar que la Dirección de Gestión y Control Interno, si trabajó de la mano con la Dirección de Informática y Estadística, con la Dirección Ejecutiva y con otras Direcciones del RENAP el Plan de Continuidad de Negocios, tal y como lo establece el artículo 46 del Decreto 90-2005, como dependencia encargada de la formulación de planes y programas institucionales.

En este sentido, la Dirección de Gestión y Control Interno, a través de la Subdirección de Control y el Departamento de Organización y Métodos, trabajó en la elaboración del instrumento Política de Continuidad del Negocio Norma UNE -EN-ISO- 22301: 2015, de la cual, se presenta una copia y el instrumento Alcance del Sistema de Gestión de Continuidad del Negocio Óptica UNE-EN-ISO 22301: 2015. Como puede verse, ambos documentos que fueron aprobados por la Dirección Ejecutiva.

Así mismo, se elaboró el instrumento Plan de Continuidad del Negocio del Registro Nacional de las Personas -RENAP- "Inscripción de Nacimiento Universal y Oportuno", el cual fue trasladado al Director Ejecutivo en Funciones, Ingeniera Brenda Amarilis Gramajo González, mediante oficio DGCI-01279-2016, de fecha





31 de agosto de 2016, mediante el cual se le presenta para su conocimiento y en donde se le solicita instruir en cuanto a la implementación de las actividades pendientes de realizar previo a la auditoría externa y certificación. Posteriormente, mediante oficio DGCI-1564-2016, de fecha 17 de octubre de 2017, dirigido a Director Ejecutivo en Funciones, Ingeniera Brenda Amarilis Gramajo González, en donde se hace de su conocimiento que el referido Plan se trasladó a la Dirección de Asesoría Legal con el objeto de emitir dictamen legal correspondiente, previo a ser validado por los Directores.

En conclusión, como podrá verificarse en los documentos presentados, la Dirección de Gestión y Control Interno, trabajó con las diferentes Direcciones del RENAP en la formulación del Plan de Continuidad del Negocio, hasta el día 26 de octubre de 2016, fecha en que me notificaron el Acuerdo de Remoción, razón por la cual me fue imposible darle continuidad a dicho plan. No obstante, se presentan las gestiones realizadas durante mi gestión con respecto a dicho Plan de Continuidad de Negocios".

Comentario de la Auditoría

Se confirma el presente hallazgo para el Licenciado Hector Ivan García Solorzano, quién fungió como Subdirector de Servicios Críticos del Registro Nacional de las Personas -RENAP- por el período comprendido del 16 de mayo al 21 de septiembre de 2016, en virtud que la aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Registro Nacional de las Personas -RENAP- fue posterior al periodo de la auditoria, determinando que la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- durante el periodo del 01 de enero de 2015 al 31 de octubre de 2016 realizó operaciones sin contar con una Plan de Contingencias para la Continuidad de Operaciones Informáticas aprobado por la Dirección Ejecutiva.

Se confirma el presente hallazgo para el Licenciado Eduardo Salvador Navarro Molina, quién fungió como Subdirector de Servicios Críticos del Registro Nacional de las Personas -RENAP- por el período comprendido del 16 de mayo al 21 de septiembre de 2016, en virtud que la aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Registro Nacional de las Personas -RENAP- fue posterior al periodo de la auditoria, determinando que la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- durante el periodo del 01 de enero de 2015 al 31 de octubre de 2016 realizó operaciones sin contar con una Plan de Contingencias para la Continuidad de Operaciones Informáticas aprobado por la Dirección Ejecutiva.

Se desvanece el presente hallazgo para el Licenciado Dante Antonio Avalos Aguilar, quién fungió como Director de Gestión y Control Interno del Registro Nacional de las Personas -RENAP-, por el período comprendido del 01 de enero al



25 de octubre de 2016, en virtud que la función de elaboración y aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas no le corresponde a la Director de Gestión y Control Interno del Registro Nacional de las Personas -RENAP-.

Se confirma el presente hallazgo para el Licenciado Carlos Alberto Quintana Galindo, quién fungió como Director de Informática y Estadística del Registro Nacional de las Personas -RENAP-, por el período comprendido del 01 de julio de 2014 al 01 de agosto de 2016, en virtud que la aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Registro Nacional de las Personas -RENAP- fue posterior al periodo de la auditoria, determinando que la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- durante el periodo del 01 de enero de 2015 al 31 de octubre de 2016 realizó operaciones sin contar con una Plan de Contingencias para la Continuidad de Operaciones Informáticas aprobado por la Dirección Ejecutiva.

Se confirma el presente hallazgo para el Licenciado Rudy Leonel Gallardo Rosales, quién fungió como Director Ejecutivo del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de enero de 2015 al 01 de junio de 2016, en virtud que la aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Registro Nacional de las Personas -RENAP- fue posterior al periodo de la auditoria, determinando que la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- durante el periodo del 01 de enero de 2015 al 31 de octubre de 2016, realizó operaciones sin contar con una Plan de Contingencias para la Continuidad de Operaciones Informáticas aprobado por la Dirección Ejecutiva.

Se confirma el presente hallazgo para la Licenciada Brenda Amarilis Gramajo González, quién fungió como Director Ejecutivo del Registro Nacional de las Personas -RENAP- por el período comprendido del 08 de octubre de 2015 al 31 de octubre de 2016, en virtud que la aprobación del Plan de Contingencias para la Continuidad de Operaciones Informáticas en el Registro Nacional de las Personas -RENAP- fue posterior al periodo de la auditoria, determinando que la Dirección de Informática y Estadística del Registro Nacional de las Personas -RENAP- durante el periodo del 01 de enero de 2015 al 31 de octubre de 2016 realizó operaciones sin contar con una Plan de Contingencias para la Continuidad de Operaciones Informáticas aprobado por la Dirección Ejecutiva.

Este hallazgo fue notificado con el número 6 y corresponde en el presente informe al número 4.



Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
DIRECTOR EJECUTIVO	RUDY LEÓNEL GALLARDO ROSALES	12,000.00
DIRECTOR EJECUTIVO	BRENDA AMARILIS GRAMAJO GONZALEZ	12,000.00
DIRECTOR DE INFORMATICA Y ESTADISTICA	CARLOS ALBERTO QUINTANA GALINDO	7,500.00
SUBDIRECTOR DE SERVICIOS CRÍTICOS	HECTOR IVAN GARCIA SOLORZANO	5,750.00
SUBDIRECTOR DE SERVICIOS CRÍTICOS	EDUARDO SALVADOR NAVARRO MOLINA	5,750.00
Total		Q. 43,000.00

Hallazgo No. 5

Falta de un oficial de seguridad

Condición

En el Registro Nacional de las Personas -RENAP-, se observó dentro del Organigrama Institucional del RENAP, que no se tiene implementada la figura de un Oficial de Seguridad Informático (OSI), que tenga a su cargo las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.2 Estructura de Control Interno, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, diseñar e implantar una estructura efectiva de control interno, que promueva un ambiente óptimo de trabajo para alcanzar los objetivos institucionales.

Una efectiva estructura de control interno debe incluir criterios específicos relacionados con: a) controles generales; b) controles específicos; c) controles preventivos; d) controles de detección; e) controles prácticos; f) controles funcionales; g) controles de legalidad; y, h) controles de oportunidad, aplicados en cada etapa del proceso administrativo, de tal manera que se alcance la simplificación administrativa y operativa, eliminando o agregando controles, sin que se lesione la calidad del servicio y 1.6 Tipos de Controles, establece: En el Marco Conceptual de Control Interno Gubernamental, se establecen los distintos tipos de control interno que se refiere a: Control Interno Administrativo y Control Interno Financiero y dentro de estos, el control previo, concurrente y posterior."



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Causa

El Director de Informática y Estadística y el Subdirector de Servicios Críticos no han realizado las gestiones necesarias para la creación del procedimiento que incluya a un técnico para que evalué la seguridad informática de los equipos y sistemas que administra la Dirección de Informática y Estadística.

Efecto

Riesgo que el personal técnico del Departamento de Informática y Estadística, no detecte la existencia de vulnerabilidades en la seguridad e infraestructura de red, así como en las aplicaciones utilizadas por el Registro Nacional de Las Personas.

Recomendación

El Director Ejecutivo, debe girar instrucciones al Director de Informática y Estadística y al Subdirector de Servicios Críticos para crear un procedimiento, en el cual un experto en seguridad ajeno al Departamento de Informática y Estadística, realice las evaluaciones necesarias para mitigar las posibles vulnerabilidades informáticas en la infraestructura de red y sistemas utilizadas por el Registro Nacional de Las Personas.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Eduardo Salvador Navarro Molina, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período del 16 de mayo al 21 de septiembre de 2016, expone lo siguiente: "...me permito manifestar lo siguiente:

BASE LEGAL:

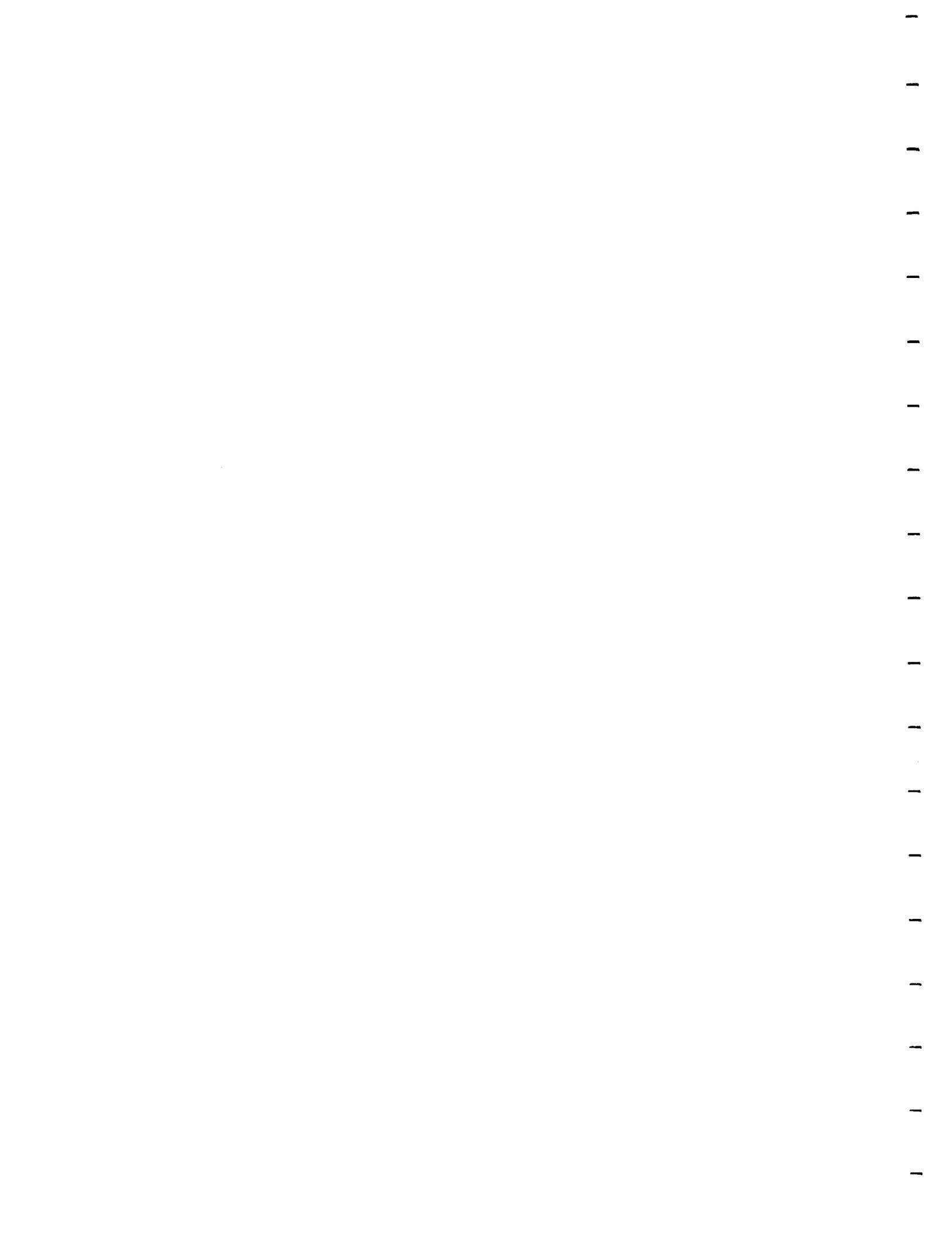
Normas Generales de Control Interno Gubernamental, emitidas por la Contraloría General de Cuentas, indica que: 2.2 ORGANIZACIÓN INTERNA DE LAS ENTIDADES... DELEGACIÓN DE AUTORIDAD: En función de los objetivos y la naturaleza de sus actividades, la máxima autoridad delegará la autoridad en los distintos niveles de mando, de manera que cada ejecutivo asuma la responsabilidad en el campo de su competencia para que pueda tomar decisiones en los procesos de operación y cumplir las funciones que les sean asignadas.

ASIGNACIÓN DE FUNCIONES Y RESPONSABILIDADES

Para cada puesto de trabajo deben establecerse en forma clara y por escrito, las funciones y responsabilidades, de tal manera que cada persona que desempeñe un puesto, conozca el rol que le corresponde dentro de la organización interna.

Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-, Artículo 50 Departamento de Seguridad Informática. Es la dependencia encargada de realizar actividades que





permitan estableceré controles de seguridad informática, por medio de evaluaciones, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información, con el fin de garantizar la disponibilidad y confidencialidad de la información.

Acuerdo de Directorio Número 82-2016, donde se aprueba "Manual de especificaciones de clases de puestos del Registro Nacional de las Personas".

ARGUMENTOS DE DESCARGO:

Se cuenta con un departamento de seguridad informática, encargado de la seguridad de software y hardware y los respectivos puestos para velar por la seguridad informática.

Durante el periodo que estuve como Subdirector de Servicios Críticos se revisaron los descriptores de puestos para los auxiliares y técnicos de sistemas de información del departamento de seguridad.

CONCLUSIÓN

De acuerdo a lo expuesto, se puede observar que el departamento de seguridad informática si cuenta con personal que tenga las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática.

DOCUMENTOS DE PRUEBA:

Normas Generales de Control Interno Gubernamental, emitidas por la Contraloría General de Cuentas.

Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-.

Organigrama del Renap

Descriptor de puestos

Auxiliar de Sistemas de Información

Técnico de Sistemas de Información

Técnico en Comunicación de Sistemas

Técnico de Sistemas.

Jefe de Seguridad Informática

PETICIÓN:

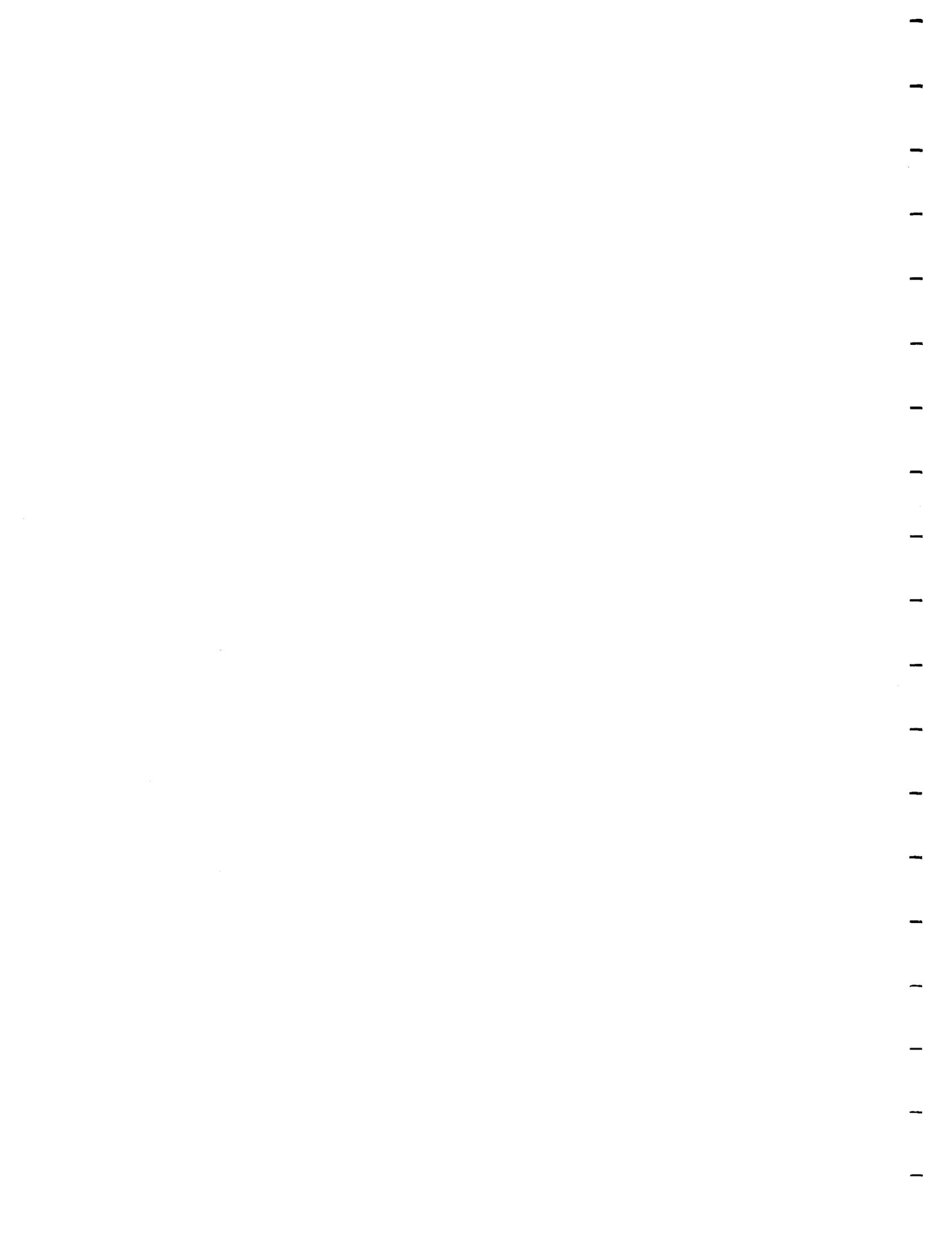
Que se valoren los documentos presentados como respaldo utilizado de base para soportar las pruebas de descargado.

Luego de su evaluación y análisis, procedan a darlos por aceptados y procedan a DESVANECER LOS POSIBLES HALLAZGOS DESCRITOS.

Se haga de mi conocimiento, la resolución final sobre el desvanecimiento del posible hallazgo comentado en esta diligencia, o se me indique las razones que le asisten a esa Comisión de Auditoría Gubernamental, para confirmar los mismos".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Héctor Iván García





Solórzano, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período del 01 de julio de 2015 al 31 de marzo de 2016, expone lo siguiente: "Yo, Héctor Iván García Solórzano, identificándome con DPI 2220 38918 0101 respetuosamente comparezco ante esta entidad contralora a evacuar la audiencia conferida y en consecuencia; hago constar que estuve en el cargo como subdirector de Servicios Críticos del 01 de julio de 2015 al 31 de marzo del 2016, presentando mi renuncia al puesto a la Dirección Ejecutiva el 28 de marzo de 2016, y se acepta mi renuncia el 31 de marzo de 2016 mediante oficio DA-SHR-dg-576-2016, haciendo constar que durante 8 meses de ocupar el puesto fue muy corto para poder evaluar y ejercer control en la subdirección de Servicios Críticos.

RAZONAMIENTO:

En la Dirección de informática y Estadística del registro de informática del Registro Nacional de las Personas, se cuenta con un Departamento de Seguridad Informática, dependencia encargada de realizar actividades que permiten establecer controles de seguridad informática, y dentro de ellas específicamente se encuentran la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información, con el fin de garantizar la disponibilidad y confidencialidad de la información, dicha estructura organizacional es acorde a las necesidades propias de la institución.

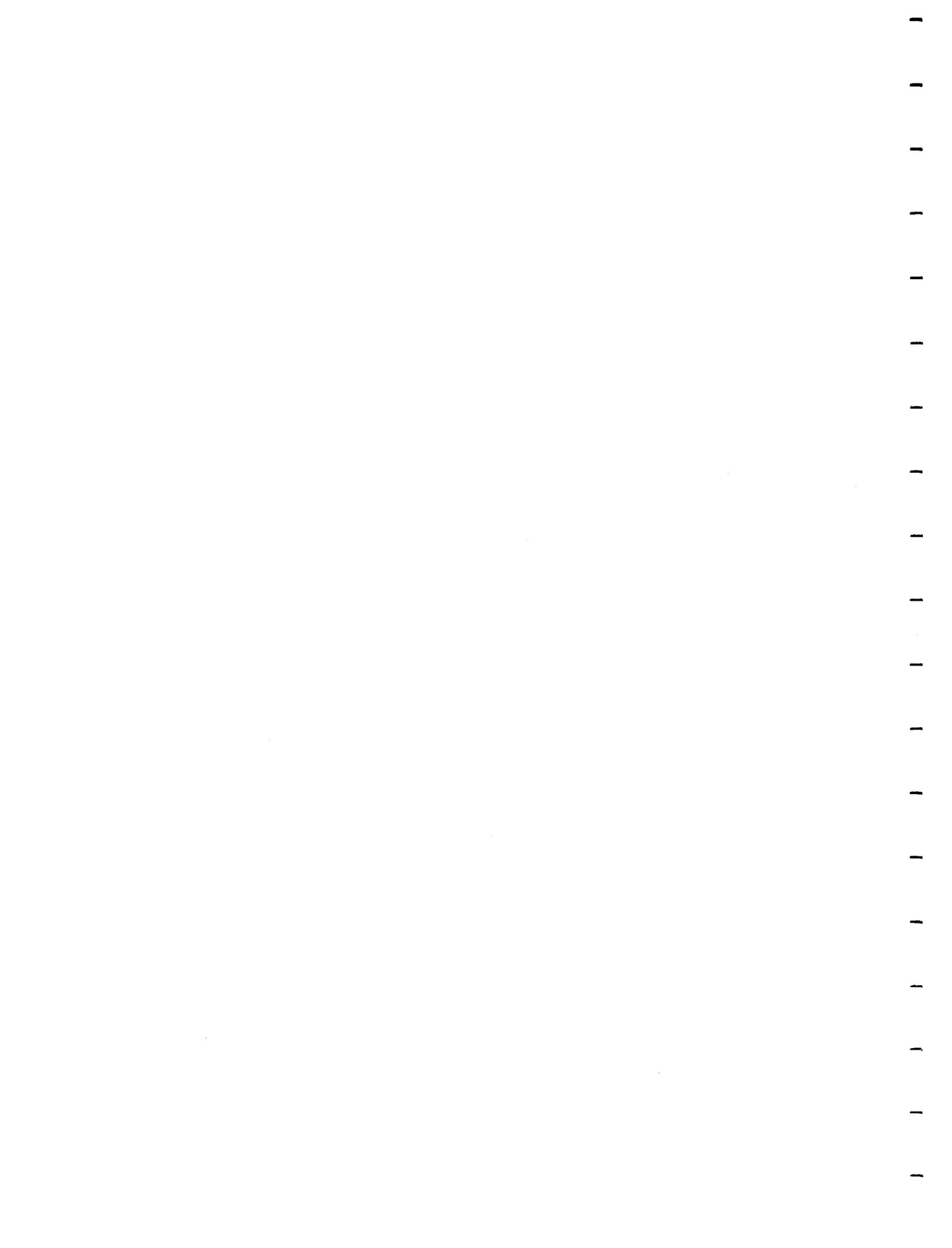
Cabe hacer mención que el jefe del departamento de seguridad informática, realiza las tareas dentro del Registro Nacional de las Personas relacionadas a la evaluación, análisis, prevención y detección de vulnerabilidades, apoyado por el personal a su cargo.

CONCLUSIÓN:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número siete (7), respecto a la "Falta de un oficial de seguridad", derivado a que si cuenta con personal específico para realizar dichas funciones".

Mediante oficio s/n y sin fecha, el señor Carlos Alberto Quintana Galindo, Director de Informática y Estadística del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 31 de octubre de 2016, indica lo siguiente: "En la Dirección de informática y Estadística del registro de informática del Registro Nacional de las Personas, se cuenta con un Departamento de Seguridad Informática, dependencia encargada de realizar actividades que permiten establecer controles de seguridad informática, y dentro de ellas específicamente se encuentran la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información, con el fin de garantizar la disponibilidad y confidencialidad de la información, dicha estructura organizacional es acorde a las necesidades propias de la institución.





Cabe hacer mención que el jefe del departamento de seguridad informática, realiza las tareas dentro del Registro Nacional de las Personas relacionadas a la evaluación, análisis, prevención y detección de vulnerabilidades, apoyado por el personal a su cargo.

PETICION:

Por los motivos indicados, solicito que se tenga por desvanecido el hallazgo número siete (7), respecto a la "Falta de un oficial de seguridad", derivado a que si cuenta con personal específico para realizar dichas funciones".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Dante Antonio Ávalos Aguilar, Director de Gestión y Control Interno del Registro Nacional de las Personas, durante el período del 01 de enero al 25 de octubre de 2016, expone lo siguiente: "De acuerdo con la condición y la causa expresada en el Hallazgo No. 7 "Falta de un oficial de seguridad", se determinó que dentro del Organigrama Institucional del RENAP, no se tiene implementada la figura de un Oficial de Seguridad Informático (OSI), que tenga a su cargo las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática. La causa es porque el Director de Informática y Estadística y el Subdirector de Servicios Críticos, no han realizado las gestiones necesarias para la creación del procedimiento que incluya a un técnico para que evalúe la seguridad informática de los equipos y sistemas que administra la Dirección de Informática y Estadística.

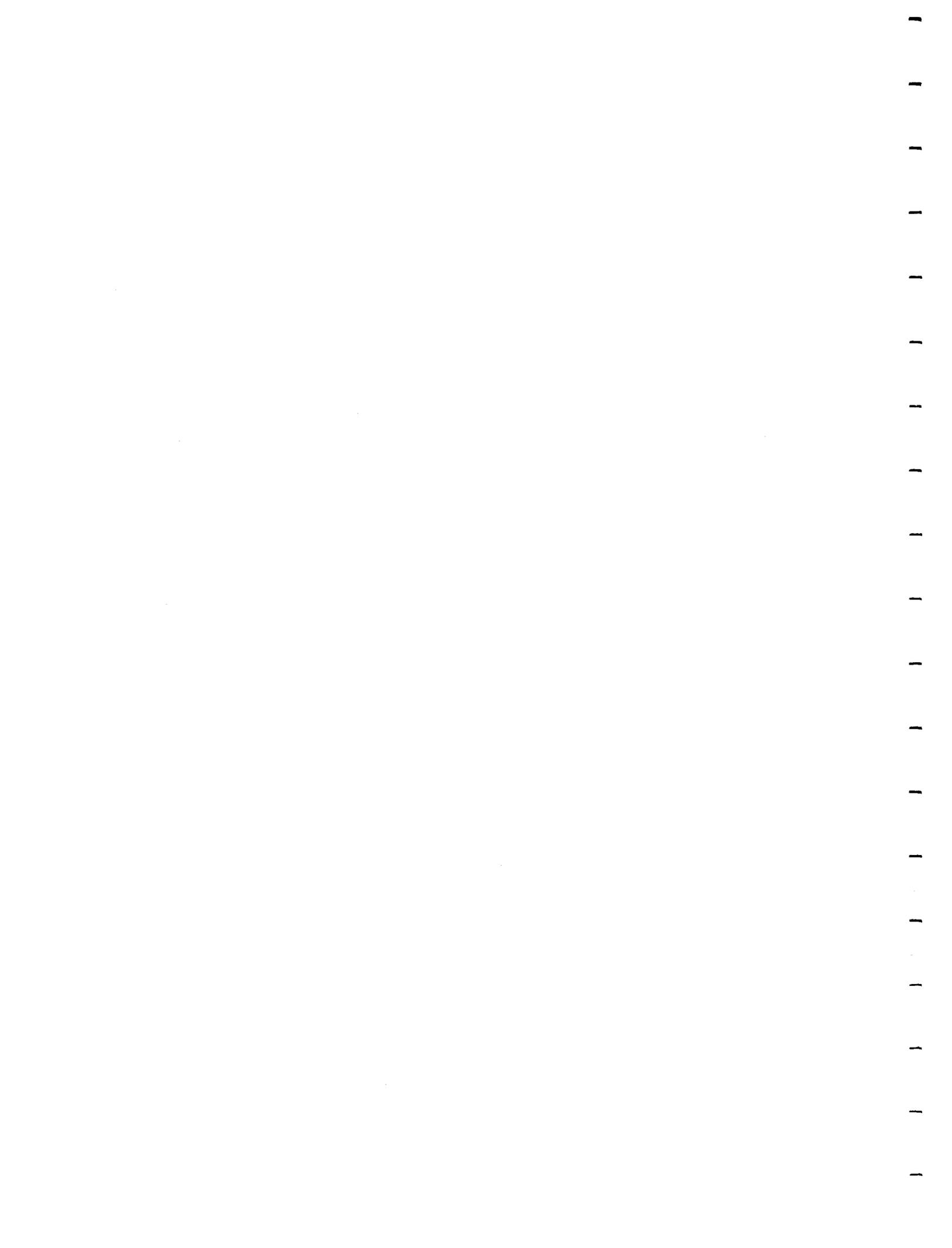
Al respecto, además de las Normas Generales de Control Interno, Norma 1.10, quiero referirme al Manual de Normas y Procedimientos establecido para el proceso de elaboración y aprobación de los Documentos Técnico Administrativos, identificado como DTA-MNP- 01- 2015, aprobado en fecha 19 de marzo de 2015. Del referido Manual, es importante en principio mencionar que fue elaborado tomando como base las Normas Generales de Control Interno Gubernamentales y al respecto, me permito citar algunas de las Normas para el diseño, elaboración y aprobación de documentos técnico administrativos.

En la norma 6.2, se establece que la máxima autoridad de cada dependencia, será responsable de que existan documentos técnico-administrativos que regulen las diferentes actividades que realizan, así como de promover y apoyar la elaboración de los mismos.

La norma 6.3, establece que el documento técnico-administrativo se elaborará con base a la información que proporcione el solicitante y/o el enlace designado.

Por otra parte, la norma 6.4 indica que la máxima autoridad de cada dependencia, será responsable de verificar y validar la información contenida en el documento





técnico administrativo que regule su actuar.

La norma 6.5 establece que la máxima autoridad de cada dependencia, será responsable de actualizar los documentos técnico-administrativos para mantener su vigencia, así como solicitar la actualización cuando corresponda.

La norma 6.6 refiere que la máxima autoridad de cada dependencia, será responsable de promover una adecuada divulgación y capacitación al personal, respecto a los documentos técnico administrativos aprobados, para su adecuada implementación y aplicación.

La norma 6.7 establece que el director o jefe de la unidad administrativa, en adelante solicitante, deberá requerir por documento oficial (oficio, memorándum, marginado, remisión, otro que deje constancia por escrito) dirigido al Director de Gestión y Control Interno, la elaboración del documento técnico-administrativo, según la necesidad a cubrir; asimismo, deberá adjuntar el formato correspondiente completo en su totalidad.

Además, la norma 6.10 establece que ...deberá programar mediante un cronograma de actividades, el documento técnico administrativo requerido, considerando los antecedentes del mismo.

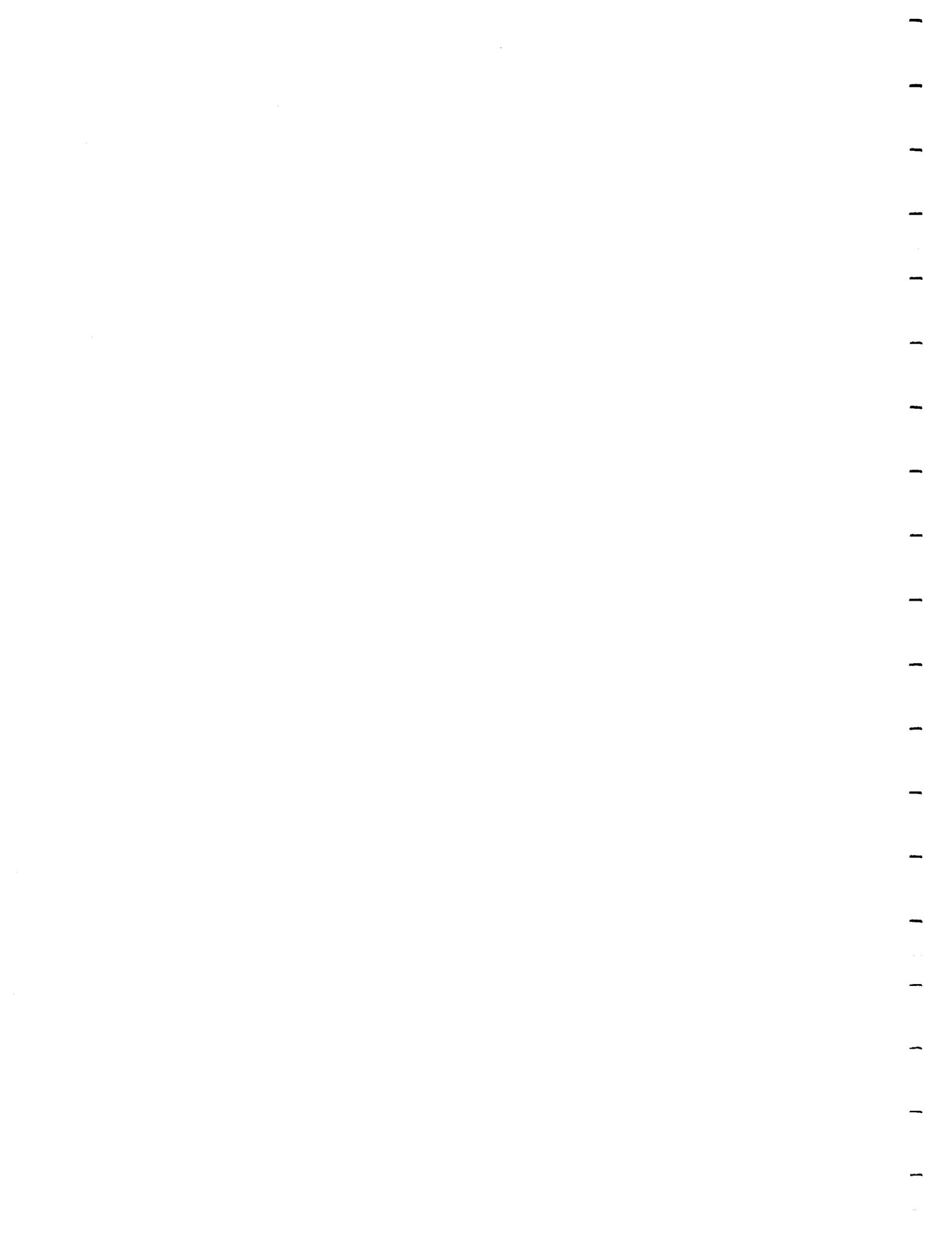
La norma 6.11 indica que ... podrá iniciar el proceso de diseño y elaboración del documento técnico-administrativo, toda vez, se haya nombrado al enlace de la contraparte y aprobado el cronograma de actividades.

En este sentido, después de haber citado las normas anteriores, quiero referirme a que la Dirección de Informática y Estadística del RENAP es la dependencia rectora en materia de almacenamiento y procesamiento de los datos, custodia y elaboración de respaldos electrónicos, así como cumplimiento de normas y mejores prácticas en materia tecnológica que garanticen su seguridad, y dentro de estos procesos se encuentra las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática.

La máxima autoridad de la Dirección de Informática y Estadística son el Director y los Subdirectores, autoridades que deben velar por que los procesos se encuentren debidamente documentados por instrumentos técnicos.

Son las máximas autoridades de la Dirección de Informática y Estadística los responsables de que los procesos de trabajo se encuentren debidamente sistematizados y documentados en instrumentos técnicos y que éstos últimos se





encuentren actualizados y de no estarlo, solicitar a la Dirección de Gestión y Control Interno el apoyo del Departamento de Organización y Métodos para que en conjunto se elaboren o actualicen dichos instrumentos técnicos.

El Director y los Subdirectores de la Dirección de Informática y Estadística tienen una responsabilidad administrativa con respecto al personal a su cargo y a la adecuada ejecución de los procesos administrativos correspondientes en materia de informática.

Las normas anteriores claramente indican la ruta administrativa correspondiente para la solicitud de documentos técnico administrativo, en este caso la creación del procedimiento que incluya a un técnico para que evalúe la seguridad informática de los equipos y sistemas que administra la Dirección de Informática y Estadística. En este sentido, la Dirección de Informática y Estadística incumplió con el envío de la solicitud dirigida al Director de Gestión y Control Interno, para la elaboración de los instrumentos correspondientes.

En conclusión, las normas anteriores indican que el procedimiento para solicitar un documento técnico administrativo e iniciar su elaboración conlleva una serie de pasos que la Dirección de Informática y Estadística no había efectuado (incumplió) hasta la fecha en que estuvo laborando en el RENAP como Director de Gestión y Control Interno, razón por la cual claramente se puede establecer que el hallazgo planteado anteriormente es responsabilidad única y absoluta del Director de Informática y Estadística, al incumplir con la normativa vigente para la solicitud y elaboración de los documentos técnico administrativos, en este caso, la actualización del referido procedimiento.

Por lo anteriormente expuesto formulo la siguiente:

PETICIÓN

Se admita para su trámite en concepto de defensa el presente informe de argumentación y los documentos adjuntos;

Se tome nota del lugar y dirección para recibir notificaciones;

Se tengan por ofrecidos los medios de prueba acompañados de los documentos presentados;

Que se tenga por evacuada en tiempo la audiencia para la discusión de los hallazgos;

Que se tengan como válidos los argumentos presentados por mi persona, en relación a los supuestos hallazgos relacionados con el Control Interno, Falta de un





Plan de Continuidad de Negocio BCP y Falta de un Oficial de Seguridad;

Que se declaren improcedentes los supuestos hallazgos notificados a mi persona;

En consecuencia, se tenga por desvanecidos los supuestos hallazgos notificados y se concluya que no soy responsable del incumplimiento de las normas generales de control interno;

Que con los argumentos expuestos y los documentos anexos como pruebas de descargo se tengan por desvanecidos los hallazgos referidos en el oficio CGC-RENAP-NOT-004-2018, de conformidad con los términos expresados en el presente memorial y que oportunamente se me notifique que han sido desvanecidos”.

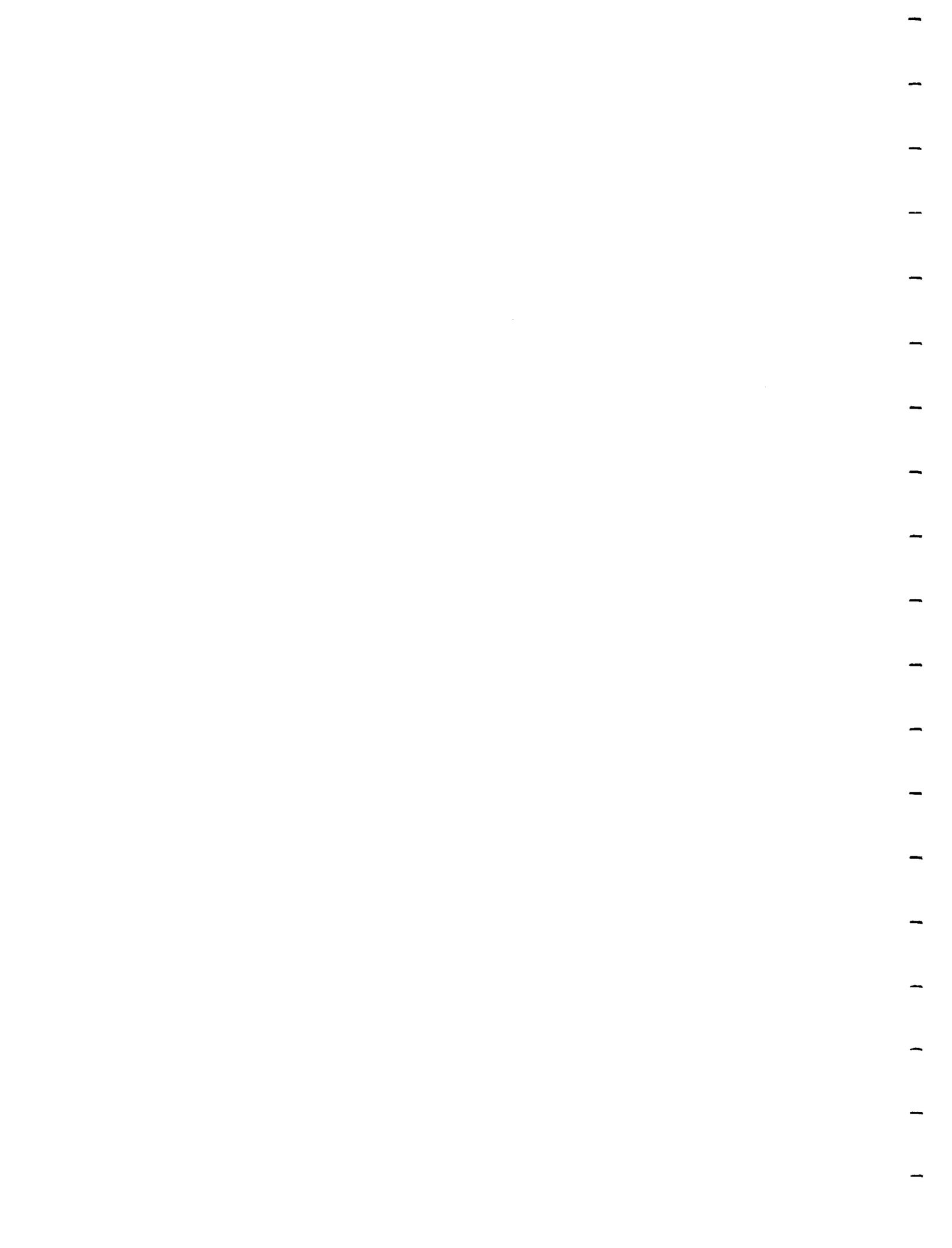
Comentario de la Auditoría

Se confirma el presente hallazgo para el señor Eduardo Salvador Navarro Molina, quién fungió como Subdirector de Servicios Críticos del Registro Nacional de las Personas -RENAP- por el periodo comprendido del 16 de mayo al 21 de septiembre de 2016, en virtud que aunque se cuenta con un departamento de seguridad informática, organizacionalmente el oficial de seguridad debe estar en un área independiente que dependa de la máxima autoridad de la entidad, o en su defecto contratar a un proveedor que realice las evaluaciones necesarias, así el trabajo realizado por el Oficial de Seguridad Informático (OSI) o el proveedor debe de ser un trabajo independiente y objetivo que permita asesorar y dar acompañamiento en la implementación de la seguridad informática del Registro Nacional de las Personas -RENAP-, así como para garantizar la disponibilidad y confidencialidad de la información.

Se confirma el presente hallazgo para el señor Hector Iván García Solórzano, quién fungió como Subdirector de Servicios Críticos del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de julio 2015 al 31 de marzo de 2016, en virtud que aunque se cuenta con un departamento de seguridad informática, organizacionalmente el oficial de seguridad debe estar en un área independiente, que dependa de la máxima autoridad de la entidad, o en su defecto contratar a un proveedor que realice las evaluaciones necesarias, así el trabajo realizado por el Oficial de Seguridad Informático (OSI) o el proveedor debe de ser un trabajo independiente y objetivo que permita asesorar y dar acompañamiento en la implementación de la seguridad informática del Registro Nacional de las Personas -RENAP-, así como para garantizar la disponibilidad y confidencialidad de la información.

Se confirma el presente hallazgo para el señor Carlos Alberto Quintana Galindo, quién fungió como Director de Informática y Estadística del Registro Nacional de





las Personas -RENAP- por el período comprendido del 01 de enero de 2015 al 31 de octubre de 2016, en virtud que aunque se cuenta con un departamento de seguridad informática, organizacionalmente el oficial de seguridad debe estar en un área independiente que dependa de la máxima autoridad de la entidad, o en su defecto contratar a un proveedor que realice las evaluaciones necesarias, así el trabajo realizado por el OSI o el proveedor debe de ser un trabajo independiente y objetivo que permita asesorar y dar acompañamiento en la implementación de la seguridad informática del Registro Nacional de las Personas -RENAP-, así como para garantizar la disponibilidad y confidencialidad de la información.

Se desvanece el presente hallazgo para el señor Dante Antonio Ávalos Aguilar, quién fungió como Director de Gestión y Control Interno del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de enero al 25 de octubre de 2016, en virtud que la función de gestionar la implementación de un oficial de seguridad es responsabilidad del Director de Informática y Estadística y también del Subdirector de Servicios Críticos del Registro Nacional de las Personas -RENAP-.

Este hallazgo fue notificado con el número 7 y corresponde en el presente informe al número 5.

Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
DIRECTOR DE INFORMATICA Y ESTADISTICA	CARLOS ALBERTO QUINTANA GALINDO	7,500.00
SUBDIRECTOR DE SERVICIOS CRITICOS	HECTOR IVAN GARCIA SOLORZANO	5,750.00
SUBDIRECTOR DE SERVICIOS CRITICOS	EDUARDO SALVADOR NAVARRO MOLINA	5,750.00
Total		Q. 19,000.00

Hallazgo No. 6

Falta de seguridad y condiciones apropiadas en el área de trabajo

Condición

En el Registro Nacional de las Personas -RENAP-, la comisión de auditoría a sistemas informáticos, determinó que no se cuenta con las medidas de seguridad mínimas en el ingreso al área restringida del Departamento de Control de Calidad, en donde se resguardan físicamente los DPI personalizados, las cuales se describen a continuación:

1. No se cuenta con una puerta que aisle la unidad catalogada como área





restringida.

2. No cuenta con el sistema de cámaras de circuito cerrado de televisión -CCTV-.
3. Carecen de extintores en el área y existe material inflamable como cajas de cartón, cajas y bolsas plásticas de empaque para los DPI.
4. No se cuenta con una caja de seguridad, en donde se resguarden documentos de valor, como serían los DPI impresos.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 1.2 Estructura de Control Interno, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, diseñar e implantar una estructura efectiva de control interno, que promueva un ambiente óptimo de trabajo para alcanzar los objetivos institucionales.

Una efectiva estructura de control interno debe incluir criterios específicos relacionados con: a) controles generales; b) controles específicos; c) controles preventivos; d) controles de detección; e) controles prácticos; f) controles funcionales; g) controles de legalidad; y, h) controles de oportunidad, aplicados en cada etapa del proceso administrativo, de tal manera que se alcance la simplificación administrativa y operativa, eliminando o agregando controles, sin que se lesione la calidad del servicio."

Causa

El Director Ejecutivo, el Director y Sub Director de Procesos el Director Administrativo y el Jefe del Departamento de Control de Calidad, no han realizado las gestiones necesarias para mejorar la seguridad y privacidad del área restringida del Departamento de Control de Calidad.

Efecto

Riesgo de extravío o sustracción de los Documento de Identificación Personal ya personalizados, debido a que la unidad no esta aislada y no se cuenta con una caja de seguridad, en donde se resguarden los DPI.

Recomendación

El Directorio debe girar sus instrucciones al El Director Ejecutivo, al Director y Sub Director de Procesos y al Director Administrativo, para crear las condiciones necesarias de seguridad para mantener el área restringida donde se localizan los Documentos de Identificación Personal ya emitidos, para su revisión por parte del Departamento de Control de Calidad.





Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Karina Floridalma Ochoa Cristales, Jefe de Control de Calidad del Registro Nacional de las Personas, durante el período del 15 al 29 de diciembre de 2015 y del 4 al 06 de enero de 2016, manifiesta: "Según oficio DA-SDRRHH-DB-2669-2015 fui notificada del nombramiento como Jefe de Control de Calidad en Sede RENAP, de la Dirección de Procesos, a partir del 1 de diciembre del 2015, cumpliendo con actividades administrativas, posteriormente fui notificada, según oficio DA-SRH-dg-2765-2015, con fecha 14 de diciembre de 2015, que se me designaba de manera temporal, con las responsabilidades, funciones y salario, inherentes al cargo de Director de Procesos, de la Dirección de procesos, durante el período comprendido del 15 al 29 de diciembre del 2015 y del 4 al 6 de enero del 2016.

En el año 2016, según el acta 13-2016, a partir del 1 de enero de 2016, estuve en el cargo de Jefe de Análisis y Verificación, fui notificada del Acuerdo de Dirección Ejecutiva 8-2016, en el cual se me otorgó el ascenso para ocupar el cargo de la Sub Dirección de Procesos a partir del 18 agosto de 2016, por motivo de salud presente mi renuncia al cargo, la cual fue recibida en el despacho de la Dirección Ejecutiva el 25 de agosto, la cual fue aceptada, según oficio DA-SDRRHH-dg-1719-2016.

Estuve fungiendo como Jefe de Control de Calidad 9 días hábiles, del 1 al 14 de diciembre del 2015 y como Sub Directora de Procesos 8 días hábiles, del 18 al 29 de agosto del 2016, sin embargo, al revisar el período auditado en las fechas del 1 de enero de 2015 al 31 de octubre de 2016, el Departamento de Control de calidad estaba en CIM, zona 12, siendo un espacio que contaba con altas medidas de seguridad y ordenados, habían extintores, cámaras de seguridad, los accesos a las áreas eran restringidos, aún para el ingreso de las autoridades se solicitaba autorización, así que los hallazgos podrían corresponder a la actual ubicación física del Departamento de Control de Calidad, razón por la cual solicité a la Unidad de Información Pública No.15-2019, la fecha en la cual el Departamento de Control de Calidad fue trasladado de CIM zona 12 al segundo nivel zona 7 y la fecha en la cual se cambió la ubicación del segundo nivel al cuarto, ya que son datos importantes y que desconozco, porque no pertenecía a la institución cuando se realizaron, la respuesta la dan en aproximadamente en 15 días.

La Dirección Administrativa debe tener los registros de las auditorías físicas realizadas al CIM, en las fechas de la auditoría".

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Rudy Leonel Gallardo Rosales, Director Ejecutivo del Registro Nacional de las Personas, durante el período comprendido del 01 de enero del 2015 al 01 de junio del 2016, manifiesta: "Exponen los auditores, que en el RENAP, se determinó que no se cuenta con las



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

medidas de seguridad mínimas en el ingreso al área restringida del Departamento de Control de Calidad en donde se resguardan físicamente los DPI personalizados, consistentes en: a) No cuenta con puerta que aisle la unidad catalogada como área restringida; b) no cuenta con cámaras de circuito cerrado -CCTV-; c) Carecen de extinguidores en el área y existe material inflamable; y, d) No cuenta con caja de seguridad para resguardar documentos de valor, como el caso de los DPI impresos.

Argumentos de Descargo:

De conformidad con el contrato 55-2008 suscrito entre el RENAP y la entidad EASY MARKETING, SOCIEDAD ANÓNIMA, el centro de impresión se encontraba bajo la responsabilidad directa de dicha entidad, puesto que específicamente dentro de sus funciones contractuales estaba la impresión del DPI, y de hecho, hasta el 2 de junio de 2016, fecha en la cual fui sustituido interinamente en el cargo por la Ingeniera Brenda Amarilis Gramajo, el Departamento de Control de Calidad estaba ubicado en el Centro de Impresión de la Zona 12, a cargo de dicha entidad mercantil, la cual contaba en ese momento con puertas metálicas de acceso, seguridad privada en los alrededores, ingreso mediante tarjeta electrónica, con cámaras de seguridad de circuito cerrado. Ahora bien, después del 2 de junio de 2016 antes indicado, entiendo que el RENAP adquirió impresora propia y se empezó a trasladar la operación de impresión a la sede central ubicada en la zona siete de la ciudad de Guatemala, pero todo ello fue realizado posteriormente a que yo dejé temporalmente el cargo, en virtud de estar detenido por orden judicial desde el 2 de junio de 2016 a la presente fecha, por lo que no tengo responsabilidad alguna en el hallazgo en mención.

Pruebas de descargo en cuanto a este hallazgo:

Contrato 55-2008 celebrado en el año 2008 por la entidad EASY MARKETING, SOCIEDAD ANÓNIMA Y EL REGISTRO NACIONAL DE LAS PERSONAS para la impresión de DPI;

Copia del Manual de Normas y Procedimientos para el Acceso Físico al data Center;

Copia del Acta de Directorio número 32-2016 del Directorio del Registro Nacional de las Personas, de fecha 2 de junio de 2016, en cuyo punto TERCERO, (PEMAS) 3.1. Se discutió el aviso que entregué en esa misma fecha haciendo ver de mi detención por orden judicial, y motivo por el cual en ese mismo punto, dicho Directorio nombraron a la Ingeniera Brenda Amarilis Gramajo González para que a partir del 2 de junio de 2016 desempeñe de manera interina el cargo de Director Ejecutivo en Funciones del RENAP.



Peticiones:

Que se tenga por presentados de mi parte los argumentos legales y pruebas de descargo correspondientes; Que se proceda a evaluar las argumentaciones vertidas de mi parte; Que una vez evaluadas las argumentaciones y pruebas de descargo, se tenga por DESVANECIDOS los hallazgos relacionados, por las razones ya argumentadas de mi parte; Que se sirvan notificarme el desvanecimiento de los referidos hallazgos”.

Mediante oficio s/n de fecha 16 de enero de 2019, el señor Julio Boanerges Ríos Contreras, Jefe de Control de Calidad del Registro Nacional de las Personas, durante el período comprendido del 16 de febrero al 31 de octubre del 2016, manifiesta: “En el periodo de tiempo del cual fui informado por medio del oficio No. CGC-RENAP-NOT-012-2018 que se realizaría la auditoria correspondiente del primero de enero de dos mil quince al treinta y uno de octubre de dos mil dieciséis, me corresponde informar que fui Jefe de Control de Calidad a partir del día dieciséis de febrero de dos mil dieciséis, como prueba de este periodo de tiempo adjunto el nombramiento numero veintidós guion dos mil dieciséis, del libro de actas de toma de posesión del personal contratado por el renglón presupuestario cero once.

Desconozco la ubicación actual del Departamento de Control de Calidad de la Dirección de Procesos, en la cual se realizó la auditoria por parte de ustedes.

En el período de tiempo en el que ustedes debían auditar, el Departamento de Control de Calidad de la Dirección de Procesos estaba ubicado en Calzada Atanasio Tzul 22-00 Centro Empresarial El Cortijo 2 Bodega 119, zona 12 de la Ciudad de Guatemala, en dichas instalaciones nos encontrábamos en el segundo nivel, cabe mencionar que se compartía las instalaciones con la empresa que proveía el servicio de impresión del Documento Personal de Identificación DPI.

En dichas instalaciones se contaba con medidas de seguridad para el personal, instalaciones y así como para los Documentos Personales de Identificación DPI, dichas medidas se detallan a continuación: Restricción de personas ajenas al departamento y a las instalaciones, solo podían ingresar al Departamento de Control de Calidad con autorización de la Dirección de Procesos y el Jefe de Control de Calidad; Cámaras de circuito cerrado de televisión en todas las instalaciones, incluyendo el Departamento de Control de Calidad tanto dentro como fuera del mismo; Monitoreo permanente (24 horas), con reportes de inconsistencias; Tarjeta electrónica de ingreso y egreso a las instalaciones, así como también al Departamento de Control de Calidad. Dicha tarjeta era única y exclusiva para cada uno de los colaboradores. Dicha tarjeta con accesos era solicitada a la empresa que proveía el servicio de impresión; El personal que laboraba en el Departamento de Control de Calidad tenía restringida la entrada a



otras áreas que no correspondieran a su departamento; Área de lockers fuera del Departamento de Control de Calidad donde se almacenaban todas las pertenencias personales, el ingreso al Departamento era solo con su uniforme; Espacio asignado y exclusivo para la recepción y almacenamiento de los Documentos Personales de Identificación DPI; Caja fuerte de seguridad exclusiva para el Departamento de Control de Calidad; Puerta blindada para acceso al Departamento de Control de Calidad; Extintores para control de conatos de incendios; Detectores de humo en las instalaciones; Aire condicionado monitoreado y controlado; Por último se menciona que todos estos controles eran administrados por la empresa que proveía el servicio de impresión de Documentos; Personales de Identificación DPI. Todo esto de acuerdo al contrato administrativo 55-2008 el cual estaba vigente en ese periodo de tiempo.

...Prueba:

Nombramiento como Jefe de Control de Calidad de la Dirección de Procesos a partir del día dieciséis de febrero de dos mil dieciséis, acta numero veintidós guion dos mil dieciséis del Libro de Actas de toma de Posesión del Personal Contratado por el Renglón Presupuestario 011.

Oficio sin número con fecha siete de enero del presente con solicitud de información al Registro Nacional de las Personas.

Petición:

Que, de conformidad con lo argumentado, medios de prueba y fundamento de ley, se resuelva y se tenga por desvanecido el posible hallazgo número ocho (08) manifestado por la Contraloría General de Cuentas. Archivando en definitiva el supuesto hallazgo”.

Mediante oficio s/n de fecha 15 de enero de 2019, la señora Mónica Reneé Recinos Casanova, Director de Procesos del Registro Nacional de las Personas, durante el período comprendido del 05 de abril al 30 de junio del 2015, manifiesta: “...traslado la información relacionada al periodo durante el que fungí como Director de Procesos, respuesta a cada uno de los posibles hallazgos y la documentación relacionada:

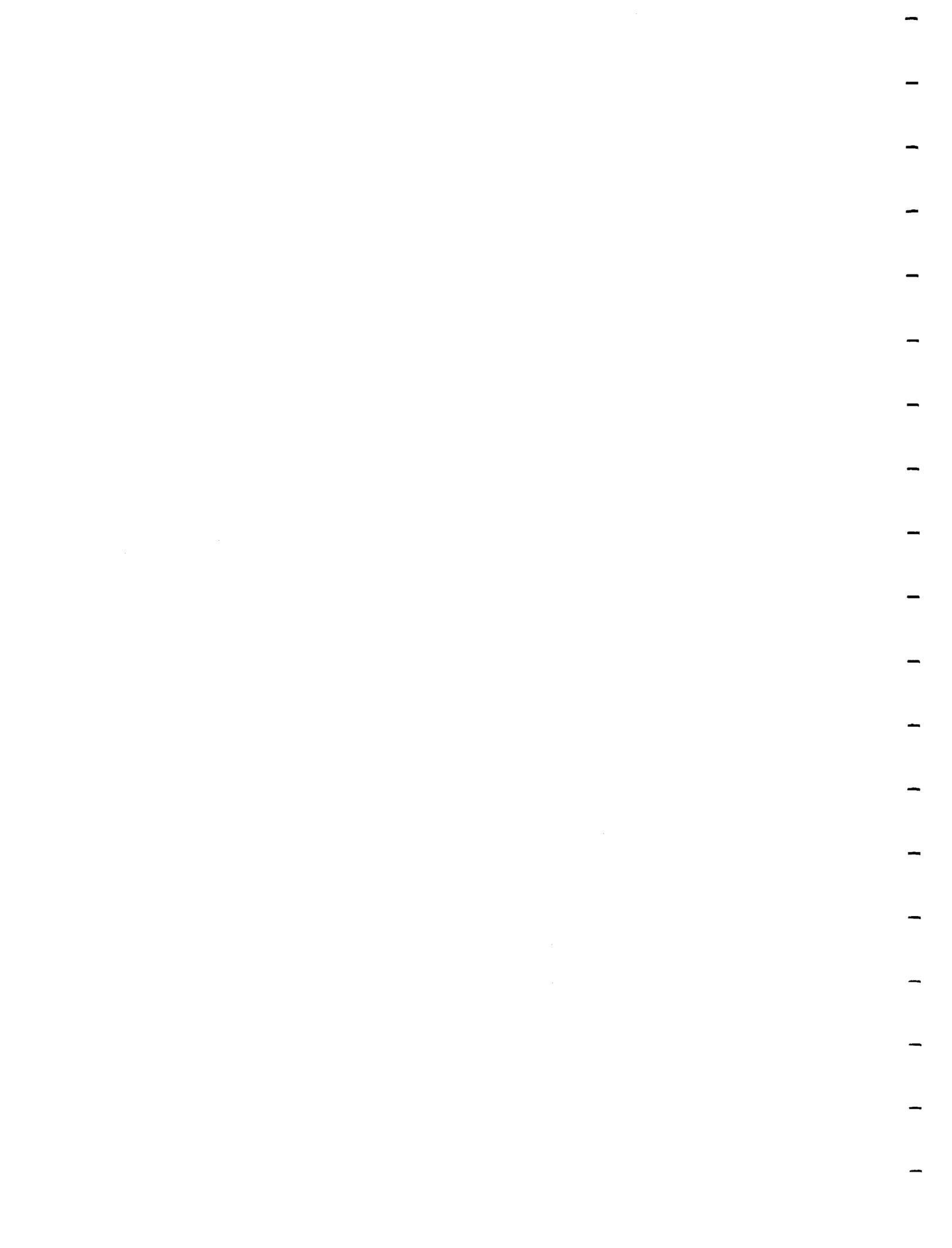
Período como Directora de Procesos

En atención al período de auditoría indicado por la comisión, y para efectos de análisis, me permito informar que fungí como Director de Procesos, durante el período del 06 de abril al 30 de junio del año 2015.

Del lugar y fecha de la Auditoría

Según oficio CGC-RENAP-NOT-018-2018 de fecha 17 de diciembre de 2018, en el cual se hace referencia al nombramiento No. DAS-12-0009-2017 de fecha 18 de





mayo de 2018, el cual fue notificado a la Dirección Ejecutiva del Registro Nacional de las Personas por oficio No. RENAP-009-OF-01-2017 de fecha 06 de octubre de 2017, mismo que fue trasladado al Subdirector de Procesos y al Director de Informática y Estadística por medio de oficio DE-6420-2017 de fecha 09 de octubre de 2017, evidenciándose que la auditoría se realizó a partir del mes de mayo de 2018, fecha en la que el Departamento de Control de Calidad y el Departamento de Impresión de la Dirección de Procesos, ya se encontraban ubicados en la Sede Central del Registro Nacional de las Personas, calzada Roosevelt 13-46 zona 7, no habiéndose realizado ninguna visita de campo a las instalaciones del Centro de Impresión -CIM- ubicado en Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, Bodega 119, 2º nivel Zona 12.

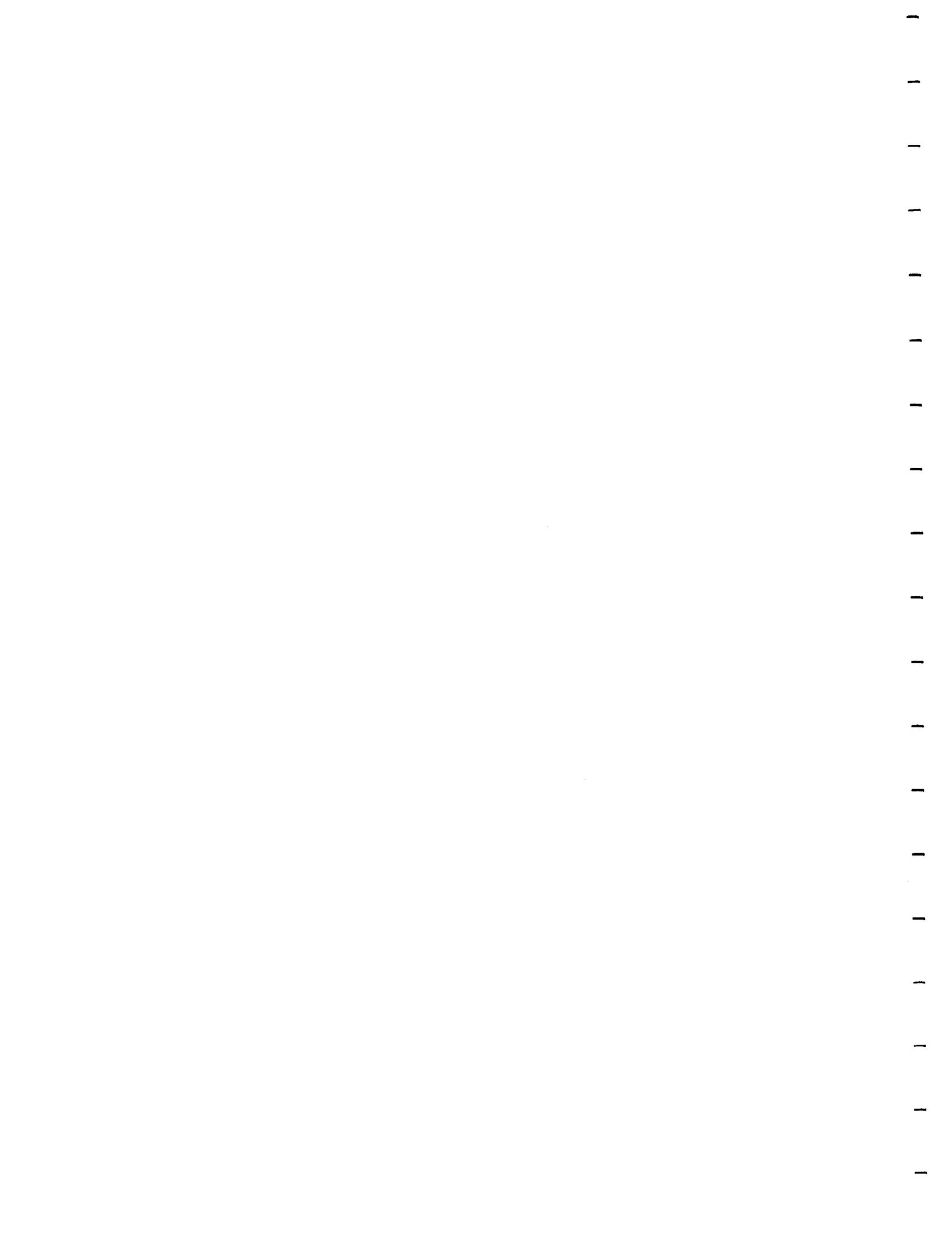
Es preciso indicar que según oficio DP-5748-2018 de fecha 28 de diciembre de 2018, de la Dirección de Procesos numeral 1: "La ubicación física del Departamento de Control de Calidad en el año 2015 era Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, Bodega 119, 2º nivel Zona 12. El ente encargado de realizar el mantenimiento a los extinguidores ubicados en dicha área era la empresa Easy Marketing, S.A., según contrato administrativo 55-2008, ya que en ese momento se encontraba vigente dicho contrato."

Asimismo, en el numeral 2 de este mismo oficio se indica: "El Departamento de Control de Calidad, fue trasladado desde febrero temporalmente con tres personas a la Sede Central del Renap, ubicado en Calzada Roosevelt 13-46, zona 7, 2º. Nivel, posteriormente en el mes de marzo del 2017 se trasladó todo el Departamento de Control de Calidad y en septiembre del mismo año fue reubicado en el 4º nivel de la instalación en mención."

En cuanto a los numerales 1, 2, 3 y 4 del presente hallazgo, en el numeral 3 del oficio DP-5748-2018: "Las instalaciones del CIM zona 12, de conformidad con lo observado contaba en ese tiempo con las siguientes medidas de seguridad: * cámaras de Circuito Cerrado * monitoreo permanente y reportes periódicos de cualquier inconsistencia * extinguidores de Polvo químico seco, * tarjeta de acceso para ingreso y egreso asignado a cada colaborador del Departamento * acceso restringido a ciertas áreas * espacio específico y restringido para la recepción de DPI * puerta blindada para el acceso al Departamento * caja fuerte de seguridad."

Lo anterior también se da en consecuencia a lo establecido en el contrato administrativo número 55-2008 de fecha 29 de diciembre de 2008, del Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relacionados, suscritos entre el Registro Nacional de las Personas -RENAP- y Easy Marketing, Sociedad Anónima, cláusula primera: "BASE LEGAL O NORMATIVA APLICABLE: La presente contratación se registrará por las disposiciones contenidas... en lo dispuesto en las Bases Administrativas





de Licitación Pública Nacional e Internacional número 02-2008 y todas sus modificaciones..., y por la oferta y las especificaciones técnicas y económicas presentadas por el contratista, documentos los cuales son considerados parte integral del presente contrato...”

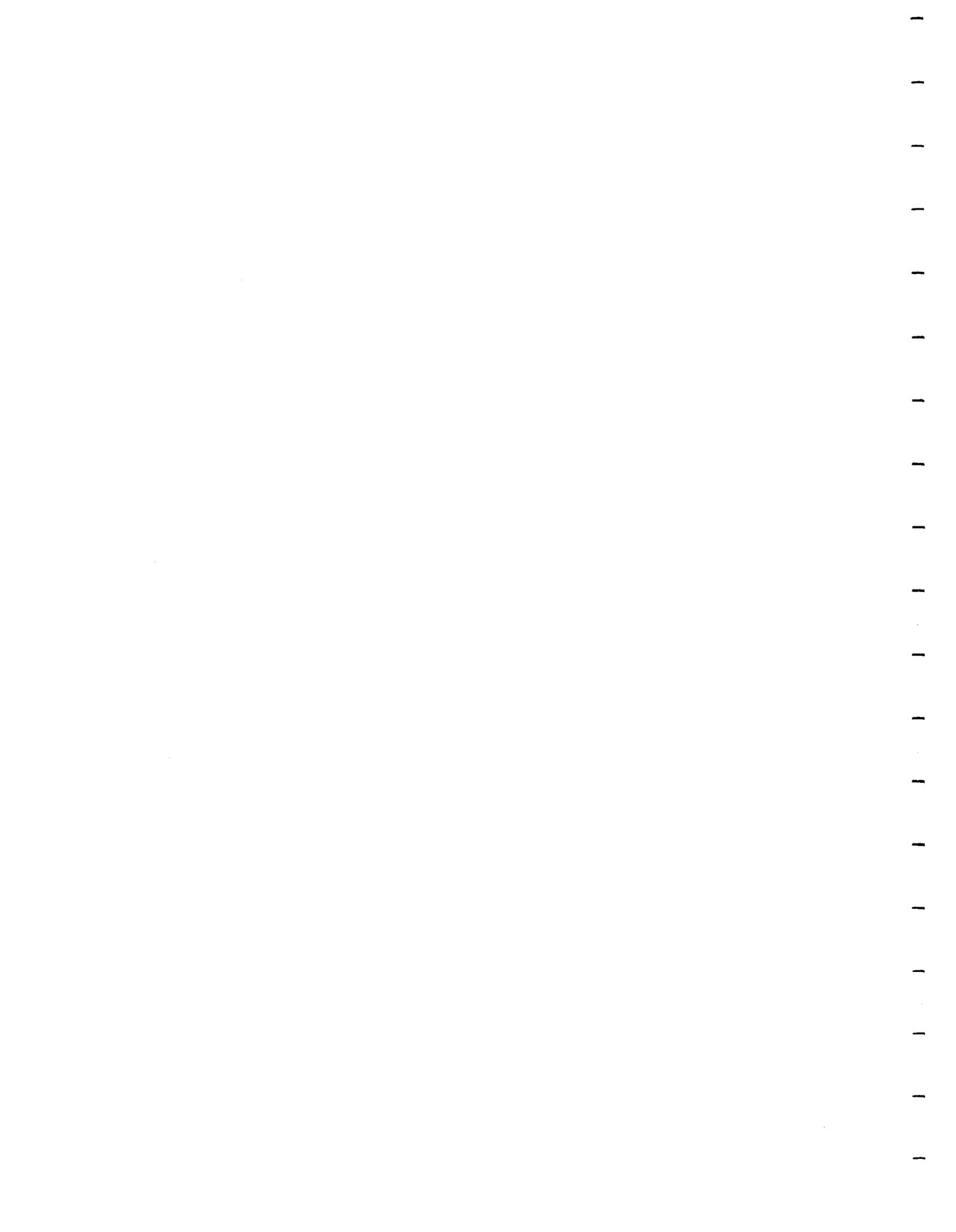
De igual forma, la Licitación Pública Nacional e Internacional 02-RENAP-2008 “Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relacionados” en el numeral 1 establece lo relacionado a las “CARACTERISTICAS BÁSICAS DE CADA CIM”, indicando: en la literal c) y d) la habilitación de un área asignada para el CIM, contemplando los elementos de seguridad como circuito cerrado, aire acondicionado, sistemas de seguridad física y en la literal e) se hace referencia a la habilitación de un área para la entrega de los documentos personalizados al personal del RENAP, además las literales f), i), j) y k) indica todo lo relacionado a las medidas de seguridad para el ingreso, circuito cerrado de televisión, sistema para control de incendios temprana mediante aspiración de aire y extinción, además del mantenimiento y soporte para todo el equipo. Y el numeral 2 relacionado al “Proceso de Personalización de DPI”, establece en la literal g) “El RENAP deberá contar con un departamento de Control de Calidad el cual pertenecerá a la Dirección de Verificación de Identidad y Apoyo Social.”. Y en el oficio sin número de fecha 30 de septiembre de 2008 suscrito por el Mandatario General con Representación Juan Carlos Pellecer Sandoval y dirigido al Registro Nacional de las Personas, en el cual se presenta la oferta presentada por el contratista, en la cual en la página número 94, apartado “ENTREGA”, establece que se contempla un área designada para hacer las entregas de DPI personalizados al RENAP, la cual correspondía al Departamento de Control de Calidad de la Dirección de Procesos, lo cual también se confirma con lo establecido en la página 131, en el apartado “RESPUESTA A LOS REQUERIMIENTOS PARA EL -CIM-” último punto.

En cuanto al resguardo de los Documentos Personales de Identificación -DPI- personalizados, los mismos eran resguardados en una caja fuerte de seguridad que se encontraba cargada a Eddie Stewart Reyes Hernández, quien se era Jefe del Departamento de Control de Calidad de la Dirección de Procesos, lo cual se comprueba por medio de Tarjeta de Responsabilidad Auxiliar, en la cual se identifica y describe la existencia del activo “Archivo de Seguridad marca Centinela” con el ID RENAP 03-1232.03-09/18.

Asimismo, los reportes y facturas de mantenimiento emitidas a la empresa Easy Marketing, Sociedad Anónima, de los meses de abril a junio del año 2015 en los que se puede evidenciar el soporte que se realizaba a las cámaras de seguridad.

Aunado a lo anterior, en el Acta de Notarial de fecha 03 de junio de 2016 en la





cual la empresa Easy Marketing, Sociedad Anónima, realiza entrega de un tomo que comprende copia simple de la constancia y carta que certifica que Easy Marketing, Sociedad Anónima ha implementado y mantenido el Sistema de Gestión de Calidad ISO 9001 ICONTEC INTERNATIONAL con fecha de vencimiento al 29 de noviembre del año 2017, por ende al contar con esta certificación ISO, el Centro de Impresión -CIM- tenía controles y procesos establecidos para la emisión del DPI, así como medidas de seguridad y condiciones apropiadas que aplicaban para el área de trabajo del Departamento de Control de Calidad.

Finalmente, en Acta Administrativa de Recepción parcial número 01-2017 de la Comisión Receptora dentro del evento de licitación pública número 02-RENAP-2008 para la Adquisición del Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relaciones, identificado con número de operación Guatecompras NOG 586595, en la cual en el punto tercero hacen constar la recepción de lo descrito en el listado proporcionado por la contratista, específicamente lo relacionado al inventario del sitio principal, el cual como ya se refirió anteriormente se encontraba ubicado en la Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, Bodega 119, 2º nivel Zona 12, lugar en el cual se encontraba ubicado el Departamento de Control de Calidad, pudiéndose evidenciar en dicha recepción, equipo de seguridad como cámaras, extintores, puerta blindada, ventana blindada, lectores de ingreso y egreso, entre otros, existiendo todas las medidas de seguridad para el área de trabajo de este departamento.

Como se puede evidenciar de forma suficiente y apropiada, el Departamento de Control de Calidad de la Dirección de Procesos, durante el periodo del 06 de abril al 30 de junio del año de 2015 durante el cual fungí como Director de Procesos, contaba con las medidas de seguridad relacionadas a: a) sistema de control de acceso compuesto de puertas blindadas y tarjetas de acceso; b) sistema de cámaras de circuito cerrado de televisión; c) extintores en todas las áreas del Centro de Impresión y sistema de supresión de incendios; y d) caja de seguridad (Archivo de Seguridad, marca Centinela) para el resguardo de los DPI impresos; siendo evidente que el posible hallazgo no corresponde a mi persona, por lo que se solicita el análisis y evaluación por parte del equipo de auditoría, a efecto de que se realice el Desvanecimiento del posible hallazgo No. 8 Falta de seguridad y condiciones apropiadas en el área de trabajo”.

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Brenda Amarilis Gramajo González, Director Ejecutivo del Registro Nacional de las Personas, durante el período comprendido del 02 de junio al 31 de octubre del 2016, manifiesta: “En relación a este hallazgo, hago constar que según certificación de fecha 11 de enero de 2019, emitida por el Jefe de Nóminas de la Subdirección de



Recursos Humanos, del Registro Nacional de las Personas, desempeñé el cargo de Director Ejecutivo en Funciones del Registro Nacional de las Personas, durante el período comprendido del 2 de junio de 2016 al 30 de junio de 2017, período en el cual tengo la absoluta certeza que el Departamento de Control de Calidad de la Dirección de Procesos, tenía en funcionamiento medidas de estricta seguridad en el ingreso al área restringida en donde se resguardaban físicamente los DPI Personalizados para lo cual detallo las medidas de seguridad que se tenían para el ingreso al área en referencia en el segundo nivel de la sede central del RENAP zona 7, ciudad de Guatemala.

Área aislada con puerta de apertura biométrica; Cámaras de circuito cerrado; Control de entradas y salidas, ya que solo el personal autorizado estaba registrado en el sistema biométrico; Monitoreo permanente y reportes periódicos de cualquier inconsistencia; Extinguidores de polvo químico seco; Tarjeta de acceso para ingreso y egreso asignado a cada colaborador del Departamento con autorización; Uso de batas y guantes apropiados para el desempeño de funciones en el control de calidad; Bóveda con ingreso biométrico donde se resguardaban las tarjetas vírgenes; Área de resguardo con cámaras de seguridad dedicadas a la vigilancia de los DPI impresos y personalizados.

Estas medidas de seguridad se encontraban vigentes y en funcionamiento durante el período que me desempeñé como Directora Ejecutiva en Funciones del RENAP, lo que certifica las medidas de seguridad y privacidad al área restringida del Departamento de Control de Calidad de la Dirección de Procesos.

Estas políticas de seguridad fueron estrictamente observadas durante mi gestión como Directora Ejecutiva en Funciones, y desconozco si el área del Departamento de Control de Calidad fue trasladada a otro lugar o nivel y si las mismas medidas continúan observándose ó si se han implementado nuevos sistemas de control.

Anterior al período como Director Ejecutivo en funciones que desempeñe, el Departamento de Control de Calidad se encontraba en el Centro de Impresión (CIM) zona 12, donde se trabajaba en conjunto con la Empresa Easy Marketing, según contrato 55-2008, lugar donde también se contaba con toda la seguridad indicada con anterioridad".

Mediante oficio s/n de fecha 04 de enero de 2019, el señor Eddie Stewart Reyes Hernández, Jefe de Control de Calidad del Registro Nacional de las Personas, por el período del 02 de marzo del 2009 al 23 de noviembre de 2015, manifiesta: "De acuerdo al período del 1 de enero del 2015 al 31 de octubre del 2016, establecido según nombramiento DAS-12-0009-2017 de fecha 18 de mayo de 2017; mi



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

desempeño al cargo como Jefe de Control de Calidad para este hallazgo se circunscribe únicamente del 1 de Enero del 2015 al 23 de Noviembre del 2015, tal como consta en:

Constancia emitida por el entonces Jefe de Nóminas del Registro Nacional de las Personas con fecha del 10 de Diciembre del 2015, en la cual se constata la finalización de labores.

Oficio DA-SRH-463-2410-2015, mediante el cual se comunica contenido del Acuerdo no. DA-SRH-463-2015-2015, de fecha 19 de noviembre del 2015, autorizado por el Director Ejecutivo del RENAP, en el que instruye de acuerdo a artículo 1, "Remover por reestructuración a Eddie Stewart Reyes Hernández del puesto de Jefe de Control de Calidad..." con fecha y hora de recibido del 23 de noviembre del 2015 a las 10:35 hrs.

Libro de Actas de Entrega de Cargo con Acta Administrativa No. 445-2015, con fecha del 23 de noviembre del 2015, mediante la cual se procede a la entrega formal del puesto de Jefe de Control de Calidad, de la Dirección de Procesos.

Constancia de Cesantía del cargo ante la Dirección de Probidad de la Contraloría General de Cuentas, formulario No. 388459, con fecha de recepción del 15 de Diciembre del 2015.

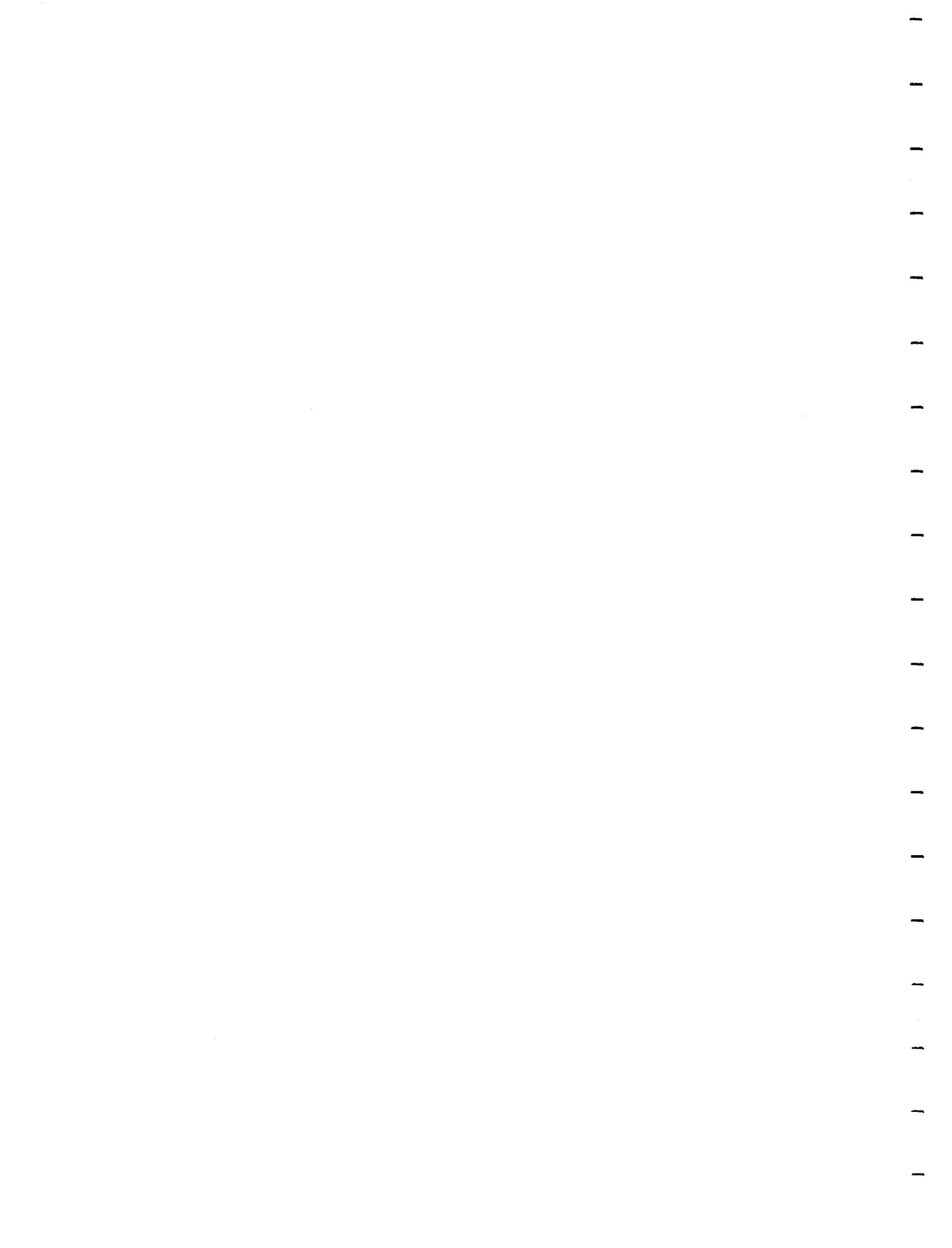
Durante el período del 1 de Enero del 2015 al 23 de Noviembre del 2015 desempeñe mi cargo como Jefe de Control de Calidad, del Departamento de Control de Calidad del Registro Nacional de las Personas, dentro de las instalaciones de CIM, las cuales estaban ubicadas físicamente en la Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, zona 12, bodega 119, 2do. Nivel, tal como consta en:

Oficio DP-5748-2018, de fecha 28 de diciembre del 2018, emitido por la Dirección de Procesos, en el que a través del numeral 1 de dicho oficio confirman que "La ubicación física del Departamento de Control de Calidad en el año 2015 era la Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, bodega 119, 2do. Nivel, zona 12.

Gafete de acceso al Centro Cortijo Empresarial II, bodega 119, entregado por Amaco Servicios, S.A.

Oficio DPR-JCC-COORDINADOR-Y-0062-2015, mediante el cual se expone que fueron recibidas físicamente y de conformidad 2 tarjetas de Acceso utilizadas por





mi persona para el acceso a las instalaciones de la bodega 119 del Cortijo Empresarial II; las cuales debían ser devueltas a la empresa Easy Marketing como administradores del sitio.

De conformidad al plazo del 1 de Enero del 2015 al 23 de Noviembre del 2015, es preciso indicar que en las instalaciones del CIM en donde se encontraba ubicado el Departamento de Control de Calidad, de la Dirección de Procesos, si se contaba con todas las medidas de seguridad en cuanto a restricciones y resguardo requeridos, según se hace constar en:

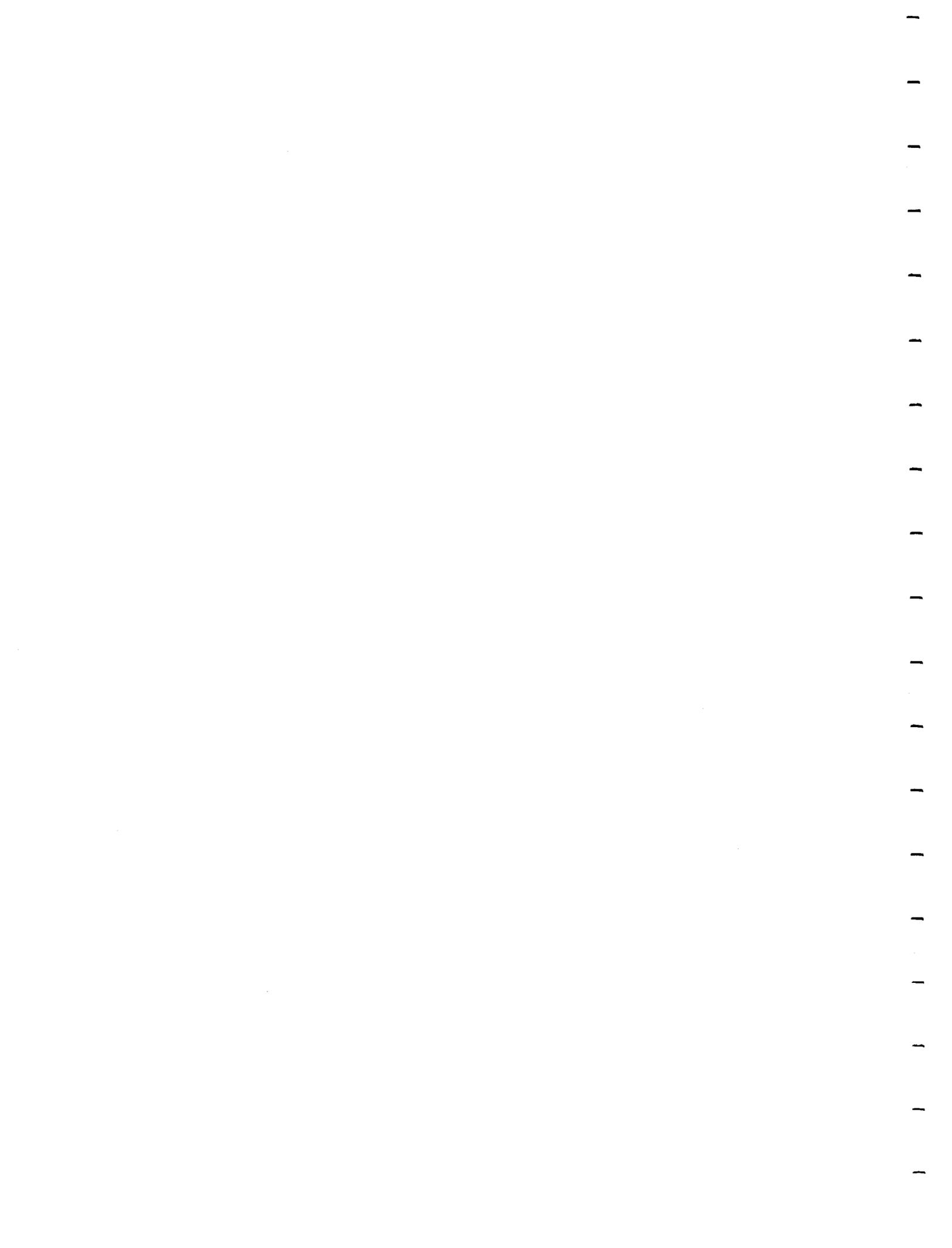
Oficio DP-5748-2018, de fecha 28 de diciembre del 2018, emitido por la Dirección de Procesos, en el que a través del numeral 3, confirman que: Las instalaciones del CIM zona 12, de conformidad con lo observado contaba en ese tiempo con las siguientes medidas de seguridad: Cámaras de circuito cerrado; Monitoreo permanente y reportes periódicos de cualquier inconsistencia; Extinguidores de polvo químico seco; Tarjeta de acceso y egreso asignado a cada colaborador del Departamento; Acceso restringido a ciertas áreas; Espacio específico y restringido para la aceptación de DPI; Puerta blindada para el acceso al Departamento; Caja fuerte de seguridad.

Tarjeta de Responsabilidad perteneciente a mi persona, en la cual se identifica y describe la existencia del activo "Archivo de Seguridad marca Centinela" con el ID RENAP 03-1232.03-09/18 utilizado para el resguardo de los -DPI-.

Que el correspondiente Oficio DP-5748-2018 es consecuencia y obedece a lo establecido en el contrato administrativo número 55-2008 de fecha 29 de diciembre de 2008, del Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relacionados, suscritos entre el Registro Nacional de las Personas -RENAP- y Easy Marketing, Sociedad Anónima, establece en la cláusula primera: "BASE LEGAL O NORMATIVA APLICABLE: La presente contratación se regirá por las disposiciones contenidas... en lo dispuesto en las Bases Administrativas de Licitación Pública Nacional e Internacional número 02-2008 y todas sus modificaciones... y por la oferta y las especificaciones técnicas y económicas presentadas por el contratista, documentos los cuales son considerados parte integral del presente contrato..."

De la Licitación Pública Nacional e Internacional 02-RENAP-2008 "Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relacionados", en el numeral 1 establece lo concerniente a las "CARACTERISTICAS BÁSICAS DE CADA CIM", indicado: en las literales "c) EL OFERENTE deberá habilitar el área asignada para la operación de cada CIM, contemplando todos los elementos de seguridad como circuitos cerrados, aires acondicionados, energía eléctrica protegida, etc. Las paredes que no sean



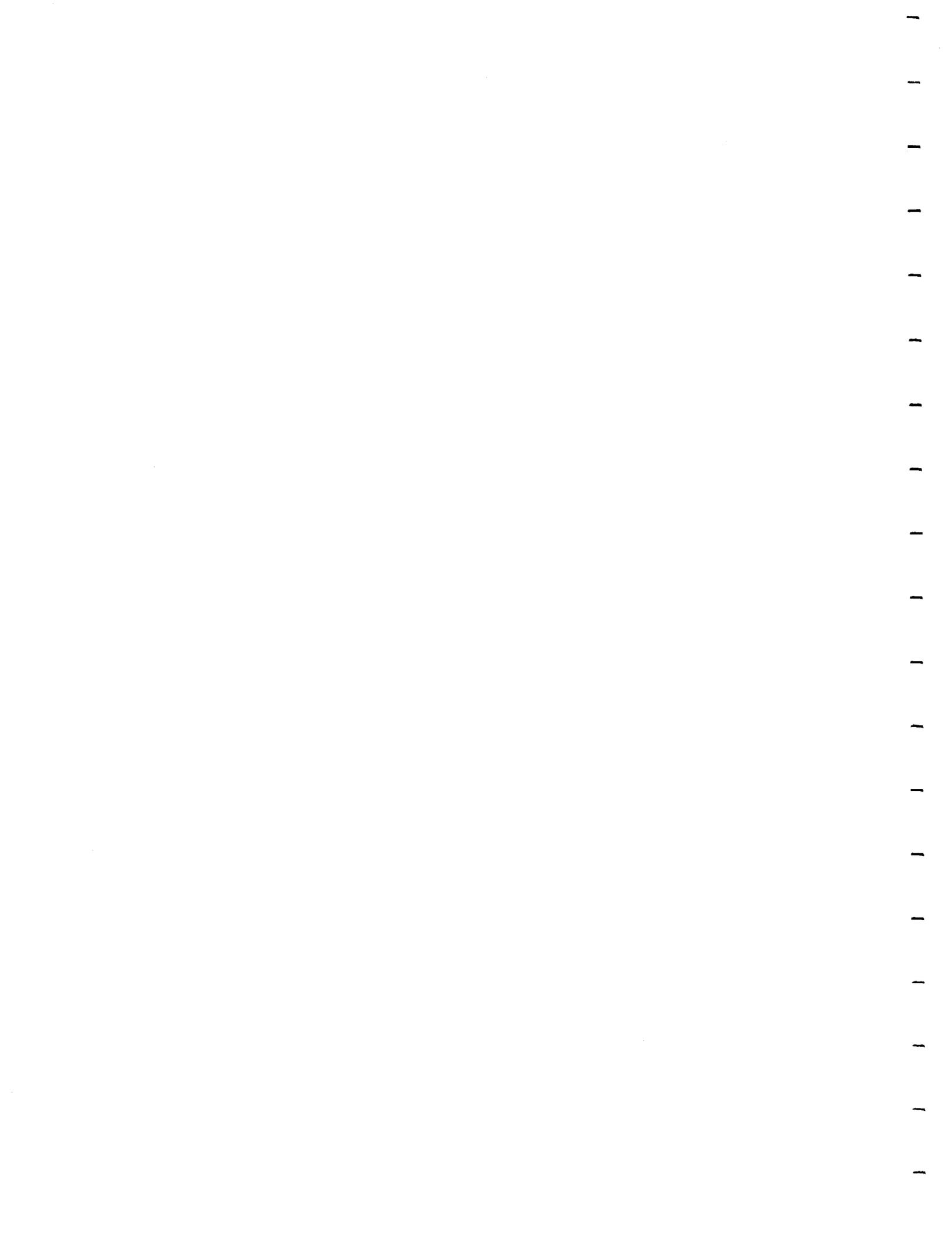


reforzadas, deberán ser acondicionadas con un mínimo de blindaje para garantizar la seguridad perimetral del CIM. Los circuitos cerrados deberán permitir la grabación continua de las actividades dentro del -CIM- y la búsqueda posterior de los videos". "d) Sistemas de seguridad física y control de acceso basados en AFIS, con sistema de auditoría avanzados y detalladas de ingresos y egresos." "e) Se deberá habilitar un área para la entrega de los documentos personalizados al personal del RENAP." "f) El ingreso al CIM deberá ser a través de un sistema de doble puerta con blindaje." "i) Sistemas de seguridad física y control de accesos basados en AFIS/FRS, con bitácoras para posterior consulta." "j) Circuito cerrado de televisión para el interior y exterior, grabación y monitoreo en color, consola de operación, cámaras panorámicas, audio, función de día/noche, activación de alarma, control remoto, grabación digital en línea para 60 días, revisión de archivos históricos, traslado de video a PC, búsqueda de eventos, resolución XGA o mejor." "k) Sistema de control de incendios de detección temprana mediante aspiración de aire y extinción con FM 200 ó similar, e instalación bajo normas de la NFPA. Se debe proveer un sistema secundario de extinguidores habilitado."

Adicionalmente en la Licitación Pública Nacional e Internacional 02-RENAP-2008 "Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relacionados", el numeral 2 relacionado al "Proceso de Personalización de DPI", establece en la literal g) "El RENAP deberá contar con un departamento de Control de Calidad el cual Pertenece a la Dirección de Verificación de Identidad y Apoyo Social.", y la oferta presentada por el contratista, en el oficio sin número de fecha 30 de septiembre de 2008 suscrito por el Mandatario General con Representación Juan Carlos Pellecer Sandoval y dirigido al Registro Nacional de las Personas, en la Parte s. Especificaciones Técnicas, 2.1 Requerimientos, "PROCESO DE EMISIÓN DEL DPI", página número 94, en el apartado "ENTREGA", establece que se contempla un área designada para hacer las entregas de DPI personalizados al RENAP, la cual correspondía al Departamento de Control de Calidad de la Dirección de Procesos, lo cual también se confirma con lo establecido en el numeral 2.1.3 "CENTRO DE IMPRESIÓN", en el apartado de "RESPUESTA A LOS REQUERIMIENTOS PARA EL -CIM-" en la página 131, último punto.

Copia de facturas emitidas a la empresa Easy Marketing, Sociedad Anónima, de los meses de abril a junio del año 2015 en los que se puede evidenciar el soporte que se realizaba a las cámaras de seguridad. Copia del Acta Notarial de fecha 03 de junio de 2016 en la cual la empresa Easy Marketing, Sociedad Anónima, a través del tercer punto literal "o" realiza entrega de un tomo que comprende copia simple de la constancia y carta que certifica que Easy Marketing, Sociedad Anónima ha implementado y mantenido el Sistema de Gestión de Calidad ISO 9001 ICONTEC INTERNATIONAL con fecha de vencimiento al 29 de noviembre del año 2017, por ende, con esta certificación ISO, el CIM contaba con la





trazabilidad y reportes necesarios para el control de las medidas de seguridad del sitio, las cuales aplicaban para el Departamento de Control de Calidad de la Dirección de Procesos que se encontraba dentro de estas instalaciones.

Finalmente, en Acta Administrativa de Recepción parcial número 011-2017 de la Comisión Receptora dentro del evento de licitación pública número 02-RENAP-2008 para la Adquisición del Sistema Integrado de Identificación e Impresión del Documento Personal de Identificación -SIDI- y Servicios Relaciones, identificado con número de operación Guatecompra NOG 586595, en la cual en el punto tercero hacen constar la recepción de lo descrito en el listado proporcionado por el contratista, específicamente en lo relacionado al inventario del sitio principal, el cual como ya se refirió anteriormente se encontraba ubicado en la Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, bodega 119, 2do. Nivel Zona 12, lugar en el cual también se encontraba ubicado el Departamento de Control de Calidad, evidenciándose en dicha recepción, equipo de seguridad como cámaras, extintores, puertas blindadas, ventana blindada, lectores de ingreso y egreso, entre otros, existiendo todas las medidas de seguridad para el área de trabajo del Departamento de Control de Calidad de la Dirección de Procesos.

Debido a que la emisión del nombramiento DAS-12-009-2017 tiene por fecha el 18 de mayo del 2017 y dicha fecha es posterior al tiempo en que desempeñe el cargo como Jefe de Control de Calidad durante el período del 1 de Enero del 2015 al 23 de Noviembre del 2015, se infiere que los hallazgos relacionados con el control interno, Área Técnica, Hallazgo No. 8, Falta de seguridad y condiciones apropiadas en el área de trabajo, fueron detectadas para el Departamento de Control de Calidad que se ubica actualmente en sede Central del RENAP, ubicado en la calzada Roosevelt 13-46, zona 7, lo cual es evidenciado a través de Oficio DP-5748-2018, de fecha 28 de diciembre de 2018, emitido por la Dirección de Procesos, en el que a través del numeral 2 confirman que desde marzo del 2017 se trasladó a todo el Departamento de Control de Calidad y en septiembre del mismo año fue reubicado en el cuarto nivel de la sede Central.

Por todo lo anteriormente expuesto, es posible determinar que los hallazgos encontrados fueron detectados en tiempo y lugar ajenos a los desempeñados por mi persona, y a que en ellos, no se hace referencia a ningún tipo de evidencia y prueba sustantiva que indique que fueron obtenidas del Departamento de Control de Calidad ubicado dentro de las instalaciones del CIM en Calzada Atanasio Tzul 22-00, Cortijo Empresarial II, bodega 119, 2º. Nivel Zona 12, por lo cual solicito el desvanecimiento de los hallazgos existentes y relacionados con el control interno, Área Técnica, Hallazgos No.8, falta de seguridad y condiciones apropiadas en el área de trabajo, para los cuales se han presentado los argumentos y



documentación de soporte que avalan el cumplimiento de cada uno de ellos y en su defecto sean atribuidos a las personas que ocupaban el cargo durante dicha auditoría en tiempo y lugar”.

Comentario de la Auditoría

Se desvanece el hallazgo, para las señoras Karina Floridalma Ochoa Cristales, quién fungió como Jefe de Control de Calidad del Registro Nacional de las Personas, por el período comprendido del 15 al 29 de diciembre del 2015 y del 04 al 06 de enero del 2016, y para Mónica René Recinos Casanova, quién fungió como Director de Procesos del Registro Nacional de las Personas, por el período comprendido del 05 de abril al 30 de junio del 2015 y Brenda Amarilis Gramajo González, quién fungió como Director Ejecutivo del Registro Nacional de las Personas, por el período comprendido del 02 de junio al 31 de octubre del 2016, en virtud que en sus comentarios y pruebas de descargo presentadas, evidencian que no tienen responsabilidad en la Falta de seguridad y condiciones apropiadas en el área de trabajo, por el breve lapso de tiempo que se encontraban como Jefe y Director en la Dirección de Control de Calidad.

Se desvanece el hallazgo, para los señores Rudy Leonel Gallardo Rosales, quién fungió como Director Ejecutivo del Registro Nacional de las Personas, por el período comprendido del 01 de enero del 2015 al 01 de junio del 2016, Julio Boanerges Rios Contreras, quién fungió como Jefe de Control de Calidad del Registro Nacional de las Personas, por el período comprendido del 16 de febrero al 31 de octubre del 2016 y Eddie Stewart Reyes Hernández, quién fungió como Jefe de Control de Calidad del Registro Nacional de las Personas, por el período del 02 de marzo del 2009 al 23 de noviembre de 2015, en virtud que en sus comentarios y pruebas de descargo presentadas, evidencian que la Dirección de Control de Calidad se encontraba a cargo de la empresa Easy Marketing, Sociedad Anónima, en el Centro de Impresión -CIM- zona 12, en donde contaba con las medidas de seguridad necesarias para el resguardo de los Documentos Personales de Identificación -DPI- impresos.

Se confirma el hallazgo, para la señora Telma Mirella Lorenzana Noriega quién fungió como Director Administrativo del Registro Nacional de las Personas, por el período comprendido del 01 de enero del 2015 al 30 de junio del 2016, debido a que fue notificada y por negligencia no se presentó a la discusión de hallazgos, no envió ningún oficio donde explicara las causas de su inasistencia o solicitara alguna ampliación o prórroga, como tampoco envió con terceros las pruebas de descargo correspondiente al hallazgo denominado Falta de Seguridad y condiciones apropiadas en el área de trabajo, en donde se emite el Documento Personal de Identificación -DPI-.



Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
DIRECTOR ADMINISTRATIVO	TELMA MIRELLA LORENZANA NORIEGA	7,500.00
Total		Q. 7,500.00

Hallazgo No. 7

Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos

Condición

En el departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, se observó que no existe un sistema de nóminas del personal y que durante los 10 años que tiene el RENAP de estar funcionando, la nómina de empleados que asciende a 2,256 empleados, se registra en hojas de cálculo Excel.

Criterio

El Acuerdo No. 09-03 del Jefe de la Contraloría General de Cuentas, en las Normas Generales de Control Interno Gubernamental, numeral 2.3 establece Sistemas de Información Gerencial, indica: "Se deben establecer y mantener sistemas de información Gerencial que produzcan información confiable y oportuna para la toma de decisiones en las unidades administrativas y puestos, de acuerdo a los roles y responsabilidades"

En el mismo cuerpo legal, en el numeral 1.6, Tipos de Controles, establece: "Es responsabilidad de la máxima autoridad de cada entidad pública, establecer e implementar con claridad los diferentes tipos de control que se relacionan con los sistemas administrativos y financieros. En el Marco Conceptual de Control Interno Gubernamental, se establecen los distintos tipos de control interno que se refiere a: Control Interno Administrativo y Control Interno Financiero, y dentro de estos, el control previo, concurrente y posterior".

Causa

El Director Ejecutivo, Director Administrativo, el Jefe del Departamento de Nóminas, no han gestionado las diligencias necesarias y oportunas para la implementación de un sistema formal de nóminas que permita llevar el control y



cálculos de los pagos efectuados al personal de la institución.

Efecto

Incertidumbre de la información del cálculo y pago de la nómina, la cual es vulnerable por estar plasmada en hojas excel, careciendo de seguridad e integridad en el manejo de la información relacionada con el pago de las nóminas del personal.

Recomendación

El Director Ejecutivo, Director Administrativo, Subdirector de Recursos Humanos y este a su vez al Jefe del Departamento de Nóminas, para que soliciten al Jefe del Departamento de Análisis de Sistemas de Información que realice el análisis y desarrollo de un sistema de nóminas, en tanto no adopten el sistema Guatenóminas.

Comentarios de los Responsables

Mediante oficio s/n de fecha 16 de enero de 2018, el señor Eduardo Salvador Navarro Molina, Subdirector de Servicios Críticos del Registro Nacional de las Personas, durante el período del 16 de mayo al 21 de septiembre de 2016, expone lo siguiente: "BASE LEGAL:

Normas Generales de Control Interno Gubernamental, emitidas por la Contraloría General de Cuentas, indica que: 2.2 ORGANIZACIÓN INTERNA DE LAS ENTIDADES... DELEGACIÓN DE AUTORIDAD: En función de los objetivos y la naturaleza de sus actividades, la máxima autoridad delegará la autoridad en los distintos niveles de mando, de manera que cada ejecutivo asuma la responsabilidad en el campo de su competencia para que pueda tomar decisiones en los procesos de operación y cumplir las funciones que les sean asignadas.

ASIGNACIÓN DE FUNCIONES Y RESPONSABILIDADES

Para cada puesto de trabajo deben establecerse en forma clara y por escrito, las funciones y responsabilidades, de tal manera que cada persona que desempeñe un puesto, conozca el rol que le corresponde dentro de la organización interna.

Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-, Artículo 68. Subdirección de Recursos Humanos. Es la dependencia encargada de los procesos de administración de puestos, reclutamiento, selección, gestión de personal, evaluación del desempeño seguridad e higiene laboral, sueldos y salarios, de conformidad con las políticas, lineamientos y disposiciones legales en materia de recursos humanos. Artículo 71. Departamento de Nóminas. Es la dependencia encargada de procesar la información del recurso humano que trabaja en la institución, para realizar los pagos y deducciones correspondientes; a fin de que





sus retribuciones le sean pagadas oportunamente, en tiempo y forma, con base a los lineamientos de las leyes decretos, reglamentos, acuerdos y otros establecidos, así como realizar otros estudios relacionados con la administración de salarios.

Acuerdo de Dirección Ejecutiva del Registro Nacional de las Personas –RENAP-, número DE-207-2017, en el cual se aprueba el Manual de Normas y Procedimientos del Departamento de Nóminas de la Dirección Administrativa de los siguientes procedimientos: a) Procedimientos para el primer ingreso (alta) del personal en el sistema de nóminas mensual de pago; b) Procedimiento para la baja del personal en el sistema de nóminas manual de pago; c) Procedimiento para movimientos del personal en el sistema de nóminas mensual de pago; d) Procedimiento para las acciones del personal en el sistema de nóminas mensual de pago; y e) Procedimiento para el emisión de nóminas mensual.

Manual de Normas y Procedimientos para el pago de las prestaciones laborales del RENAP.

ACCIONES EFECTUADAS:

Según oficio número DA-0796-2016, emitido por la Dirección Administrativa, de fecha 26 de mayo 2016, y dirigido a la Subdirección de Recursos Humanos, se dio seguimiento a la instrucción efectuada por el Director Ejecutivo respecto a la implementación del sistema informático GUATENOMINAS para el pago del personal del Registro Nacional de las Personas, RENAP, así mismo en dicha nota se sugirió efectuar reuniones con los encargados del área de pago al personal para que la implementación de dicho sistema se efectuara con urgencia.

Se realizaron varias reuniones de trabajo con el Encargado de Nóminas, para darle seguimiento a la implementación del sistema informático GUATENOMINAS, sin embargo no se presentó a la Dirección Administrativa ninguna gestión ante el Ministerio de Finanzas Públicas por parte de la Subdirección de Recursos Humanos como encargado del pago de las Nóminas para la implementación de dicho sistema.

Así mismo la Subdirección de Recursos Humanos no presentó a la Dirección Administrativa ningún requerimiento o DERCAS, para el análisis o diseño de un sistema informático para el pago de Nóminas como encargados de dicha función, según lo establecido en Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-.

CONCLUSIÓN

En cumplimiento a lo establecido en las Normas de Control Interno Gubernamental emitidas por la Contraloría General de Cuentas en relación a la Asignación de





Funciones y Responsabilidad así como la Delegación de Funciones, el RENAP con base al Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-, establece que la Subdirección de Recursos Humanos del RENAP, es el área encargada de todo lo concerniente al pago del personal, sin embargo a pesar de que la Dirección Administrativa giró la instrucción precisa de efectuar la implementación del sistema informático GUATENOMINAS, y del seguimiento dado por esta Dirección nunca se recibió de la Subdirección de Recursos Humanos, un documento que amparara las gestiones efectuadas ante el Ministerio de Finanzas Públicas para la implementación de dicho sistema, así como ningún requerimiento o DERCAS, para el análisis o diseño de otros sistema informático que pudiera ser utilizado alternativamente para el pago de Nóminas.

DOCUMENTOS DE PRUEBA:

Normas Generales de Control Interno Gubernamental, emitidas por la Contraloría General de Cuentas.

Acuerdo del Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas –RENAP-.

Acuerdo de Dirección Ejecutiva del Registro Nacional de las Personas –RENAP-, número DE-207-2017

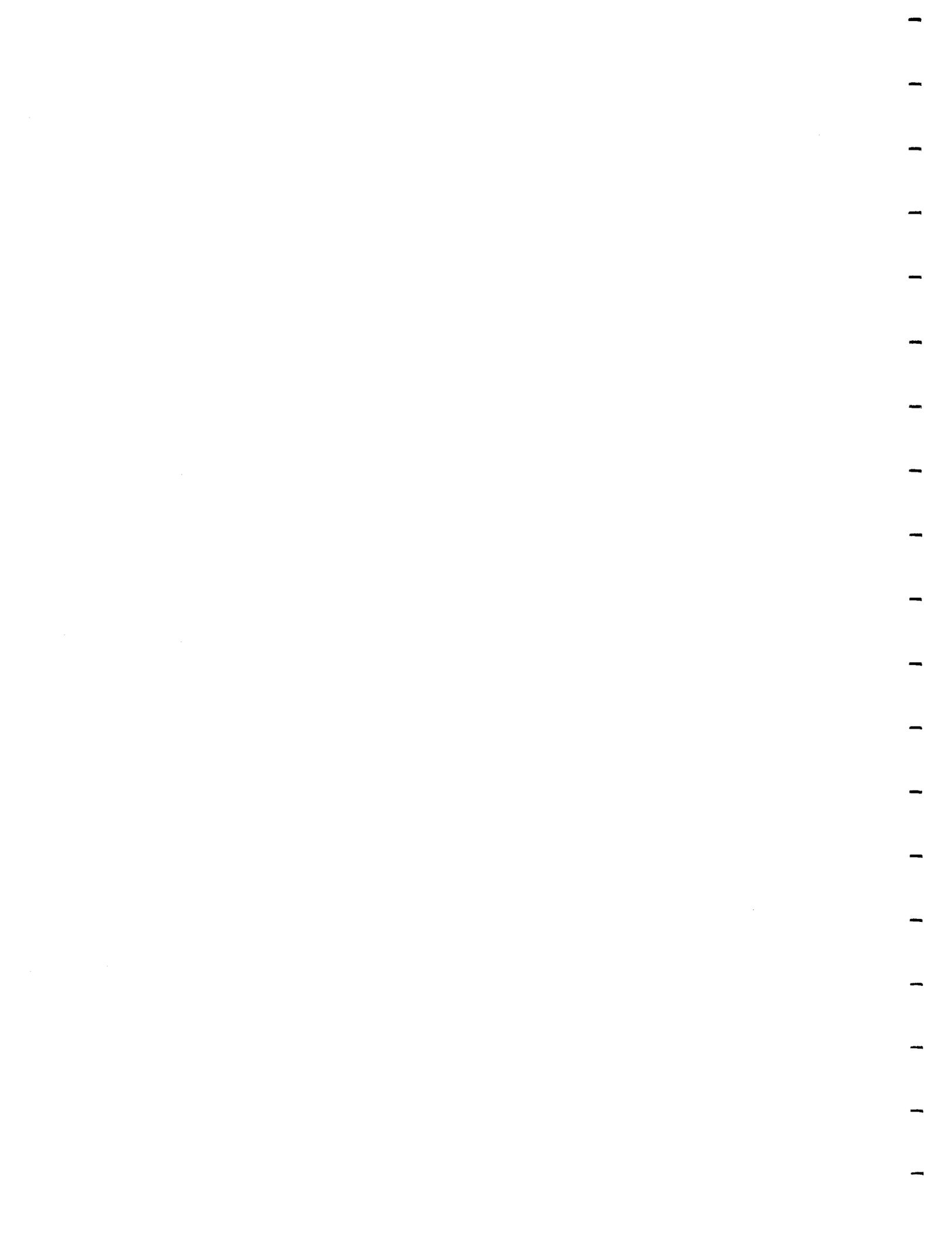
Oficio DA-0796-2016, de fecha 26 de mayo 2016.

Acta número 33-2016 de la Sub-Dirección de Recursos Humanos, Dirección Administrativa del Registro Nacional de las Personas Renap, de toma de posesión del cargo de Director Administrativo del Registro Nacional de las Personas -RENAP- del 22 de septiembre del año 2016.

Por lo anteriormente expuesto SOLICITO: se tomen en cuenta los argumentos y documentación de respaldo adjuntos al presente memorial y se deje sin efecto o se desvanezca en su totalidad Hallazgo número 11, de Control Interno Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos”.

Mediante oficio s/n de fecha 16 de enero de 2018, el señor Rony Domingo Ibáñez Ramírez, Jefe de Nóminas del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 31 de octubre de 2018 que, de acuerdo a la designación de presentarse al REGISTRO NACIONAL DE LAS PERSONAS, -RENAP- a practicar auditoría a Sistemas Informáticos, por el período comprendido del 01 de enero de 2015 al 31 de octubre de 2016, y como resultado se hace del conocimiento del hallazgo relacionado con el Control Interno: Área Técnica ; Hallazgo No. 11 “Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos”, y que como causal indican; que no han gestionado las diligencias necesarias y oportunas para la implementación de un sistema formal de nóminas que permita llevar el control y cálculos de los pagos efectuados al personal de la institución.





De acuerdo a lo anterior, se hace del conocimiento que, desde el momento de ingreso a la institución como Jefe del Departamento de Nóminas, existió la preocupación por llevar controles, registros y efectuar pagos en formato de Microsoft Excel, razón por la cual se me informó que se estaba trabajando un sistema informático denominado "Sistema Informático de RH/Nóminas Delta" pero por razones ajenas al departamento no fue posible la implementación del mismo. Por lo que se inició con la implementación del "Sistema de Nóminas y Registro de Personal -GUATENOMINAS-", el cual pertenece al Sistema Integrado de Administración Financiera -SIAF- del Ministerio de Finanzas Públicas, realizando las diligencias que a continuación se detallan:

No.	DOCUMENTO	FECHA	DILIGENCIA EFECTUADA
1	Ref. DE-2288-2014	04/09/2014	Solicitud de apoyo para la implementación del Sistema GUATENOMINAS en el departamento de Nóminas de la Subdirección de Recursos Humanos de la institución.
2	DA-SDRRHH-376-2014 y DA-SDRRHH-382-2014	26/09/2014 08/10/2014	En ambos se envió de listado de personal considerado al someterse a la capacitación del sistema, previo a la implementación de GUATENOMINAS, así como el traslado de la red programática de la Institución.
3	Oficio No. DCE-DAS-514-2014	11/11/2014	Información por parte de Dirección de Contabilidad del Estado del Ministerio de Finanzas Públicas, sobre la creación de 12 usuarios para la capacitación del sistema GUATENOMINAS.
4	Ref. DE-069-2015	09/01/2015	Solicitud de informa sobre las acciones realizadas para implementar en el RENAP, el sistema de GUATENOMINAS.
5	DA-SRRHH-247-2015	06/04/2015	Traslado de información solicitada por Auditoría Interna, con respecto al sistema de información del departamento de Nóminas de la Subdirección





			de Recursos Humanos del RENAP.
6	Contrato Administrativo de Servicios Técnicos No. 144-2015	15/04/2015	Contratación de la señorita Endy Fabiola Ajtún García, como asesora para la implementación del sistema GUATENOMINAS, según términos de referencia, (persona que estuvo bajo el mando de este servidor)
8	DA-SDRRHH-DN-291-2015	20/04/2015	Solicitud de activación de usuarios dentro del sistema GUATENOMINAS, para iniciar con las pruebas técnicas y consultas respectivas al proceso de implementación del sistema.
9	Oficio No. DCE-DAS-323-2015	24/04/2015	Información por parte del Ministerio de Finanzas Públicas, sobre activación de usuarios RDIBANEZ (Rony Domingo Ibáñez Ramírez) y EFAJTUNG (Endy Fabiola Ajtún García), en el sistema GUATENOMINAS
10	SIN CORRELATIVO	29/04/2015	Propuesta de proyecto de implementación del sistema de Nómina y Registro del Personal GUATENOMINAS en RENAP
11	DA-SDRRHH-DN-368-2015	11/05/2015	Solicitud de habilitación temporal del acceso a las páginas WEB de Gobierno de Guatemala (extensión ".gob.gt"), para la implementación del sistema de nómina GUATENOMINAS
12	SIN CORRELATIVO	28/05/2015	Informe de avances obtenidos del proyecto de implementación del sistema GUATENOMINAS
13	SIN CORRELATIVO	11/06/2015	Solicitud de Reglamento





			Orgánico Interno y Perfiles de puestos Directivos para iniciar la Etapa No. 2 del proyecto de Implementación del Sistema GUATENOMINAS
14	SIN CORRELATIVO	24/06/2015	Informe de avances obtenidos del proyecto de implementación del sistema GUATENOMINAS
15	DA-SRRHH-DN-505-2016	24/05/2016	Informe al Ministerio de Finanzas Públicas de trabajo realizado en el sistema GUATENOMINAS y solicitud de información sobre la posibilidad de implementar dicho sistema en RENAP a la brevedad posible
16	DE-15242016	24/05/2016	Solicitud de informe sobre avances de gestión de implementación del sistema de nóminas GUATENOMINAS
17	ACUERDO MINISTERIAL No. 223-2016 "A"	30/05/2016	Normativa que dicta las directrices para la implementación del Sistema de Nóminas y Registro de Personal -GUATENOMINAS- en todas las entidades del sector público no financiero.
18	DA-SDRRHH-DN-542-2016	03/06/2016	Informe de avance y logros de implementación del sistema GUATENOMINAS, así como causal por la cual no ha sido posible la continuidad de la segunda fase del proyecto de implementación.
19	DA-SRRHH-DN-841-2016	20/09/2016	Solicitud de informe sobre fase en la que se encuentra la elaboración del Reglamento Orgánico Interno de RENAP, en virtud que se debe de entregar al Ministerio de Finanzas Públicas para





		continuar con la implementación del sistema GUATENOMINAS.
--	--	---

Adicionalmente se informa que durante el período que comprende la auditoría efectuada, este servidos como Jefe del Departamento de Nóminas de RENAP, realizó las gestiones que correspondieran de acuerdo a la jerarquía del puesto, por lo que solicito de la manera más atenta sirvan considerar los documentos, para el desvanecimiento del hallazgo notificado, y que en lo que respecta a las fases subsiguientes de implementación del sistema GUATENOMINAS, no se imputan a mis responsabilidades por haber sido removido del puesto el 15 de febrero del año 2017”.

Mediante oficio s/n de fecha 16 de enero de 2018, el señor Rudy Leonel Gallardo Rosales, Director Ejecutivo del Registro Nacional de las Personas, durante el período del 01 de enero de 2015 al 01 de junio de 2016, expone lo siguiente: “Exponen los auditores, en el Departamento de Sistemas de Información del RENAP se observó que no existe un sistema de nóminas del personal y que durante los 10 años que tiene esa institución, la nómina de empleados que asciende a 2,256, se registra en hojas de cálculo Excel, indicando que el Director Ejecutivo, Director Administrativo, Subdirector de Recursos Humanos y el Jefe del Departamento de Nóminas no han gestionado diligencias necesarias y oportunas para la implementación de un sistema formal que permita llevar el control y cálculos de los pagos efectuados al personal de la institución.

ARGUMENTOS DE DESCARGO:

Primeramente debe indicarse que en materia Administrativa, existe una segregación de funciones, puesto que es humanamente imposible que el Director Ejecutivo pueda estar presentes en todas las acciones y gestiones propias de cada Dirección, Subdirección y Unidad Administrativa del RENAP. En ese contexto, la responsabilidad de dicha materia es tanto del área de Recursos Humanos, particularmente de Nóminas. Sin embargo, si bien es cierto que desde que el RENAP existe nunca se había trabajado en llevar un mejor control de nóminas, ese no es el caso de mi persona, puesto que yo sí efectué acciones oportunas, tendientes a dichos controles. En efecto, en el período auditado, coordiné con el Subdirector de Recursos Humanos y el Jefe del Departamento de Nóminas, acciones por llevar controles, registros y efectuar pagos en forma adecuada, de tal forma que se inició el trabajo con un sistema informático denominado “Sistema Informático de RH/Nóminas Delta” y además, se inició con la implementación del “Sistema de Nóminas y Registro de Personal –GUATENOMINAS-”, el cual pertenece al Sistema Integrado de Administración Financiera –SIAF- del Ministerio de Finanzas Públicas, realizando las diligencias que a continuación se detallan:





No.	DOCUMENTO	FECHA	MOTIVO
1	Ref. DE-2288-2014	04/09/2014	Solicitud de apoyo para la implementación del Sistema GUATENOMINAS en el departamento de Nóminas de la Subdirección de Recursos Humanos de la institución.
2	DA-SDRRHH-376-2014 y DA-SDRRHH-382-2014	26/09/2014 08/10/2014	En ambos se envió de listado de personal considerado al someterse a la capacitación del sistema, previo a la implementación de GUATENOMINAS, así como el traslado de la red programática de la Institución
3	Oficio No. DCE-DAS-514-2014	11/11/2014	Información por parte de Dirección de Contabilidad del Estado del Ministerio de Finanzas Públicas, sobre la creación de 12 usuarios para la capacitación del sistema GUATENOMINAS.
4	Ref. DE-069-2015	09/01/2015	Solicitud de informe sobre las acciones realizadas para implementar en el RENAP el sistema de GUATENOMINAS
5	DA-SRRHH-247-2015	06/04/2015	Traslado de información solicitada por Auditoría interna, con respecto al sistema de información del departamento de Nóminas de la Subdirección de Recursos Humanos del RENAP.
6	Contrato Administrativo de Servicios Técnicos No. 144-2015	15/04/2015	Contratación de la señorita Endy Fabiola Ajtún García, como asesor para la implementación del sistema GUATENOMINAS, según términos de referencia, (persona que estuvo a cargo de este servidor)



7	DA-SDRRHH-DN-368-2015	11/05/2015	Solicitud de habilitación temporal el acceso a las páginas WEB de Gobierno de Guatemala (extensión ".gob.gt"), para la implementación del sistema de nómina GUATENOMINAS
8	DA-SDRRHH-DN-291-2015	20/05/2015	Solicitud de activación de usuarios dentro del sistema GUATENOMINAS, para iniciar con las pruebas técnicas y consultas respectivas a proceso de implementación del sistema
9	SIN CORRELATIVO	29/05/2015	Propuesta de proyecto de implementación del sistema de Nómina y Registro de Personal GUATENOMINAS en RENAP
10	Oficio No. DCE-DAS-323-2015	24/05/2015	Información por parte del Ministerio de Finanzas Publicas, sobre activación de usuarios RDIBANEZ (Rony Domingo Ibañez Ramirez) y EFAJTUNG (Endy Fabiola Ajtún García), en el sistema GUATENOMINAS
11	SIN CORRELATIVO	28/05/2015	Informe de avances obtenidos del proyecto de implementación del sistema GUATENOMINAS
12	SIN CORRELATIVO	11/06/2015	Solicitud de Reglamento Orgánico Interno y Perfiles de puestos Directivos para iniciar la Etapa No. 2 del proyecto de Implementación del Sistema GUATENOMINAS
13	SIN CORRELATIVO	24/06/2015	Informe de avances obtenidos del proyecto de implementación del sistema GUATENOMINAS
14	DE-1524-2016	24/05/2016	Solicitud de informe sobre avances de gestión de





			implementación del sistema de nóminas GUATENOMINAS
15	DA-SDRRHH-DN-542-2016	03/06/2016	Informe de avance y logros de implementación del sistema GUATENOMINAS

Resalta el hecho que en oficio Ref DE-2288-2014 del 4 de septiembre de 2014, ya existían instrucciones de mi parte como Director Ejecutivo a ese respecto, puesto que en dicho documento solicité al Director de Tecnología de la Información del Ministerio de Finanzas Públicas, el apoyo de esa dirección para el proceso de implementación del Sistema Guatenóminas en el RENAP, por lo que el hallazgo relacionado, en cuanto a mi persona no tiene razón de ser, puesto que fue precisamente dicho oficio, el que dio inicio a las acciones antes descritas, las cuales no pude culminar, tomando en cuenta que desde el 2 de junio de 2016 fui detenido y suspendida mi relación de trabajo con el RENAP.

PRUEBAS DE DESCARGO EN CUANTO A ESTE HALLAZGO:

- Copia del oficio Ref. DE-2288-2014 de fecha 4 de septiembre de 2014;
- Copia del oficio DA-SDRRHH-376-2014 del 26 de septiembre de 2014;
- Copia del oficio DA-SDRRHH-382-2014 del 8 de octubre de 2014;
- Copia del oficio DA-SRRHH-DN-247-2015 del 6 de abril de 2015;
- Copia del oficio DA-SDRRHH-DN-452-2015 del 2 de junio de 2015.

PETICIONES:

- Que se tenga por presentados de mi parte los argumentos legales y pruebas de descargo correspondientes;
- Que se proceda a evaluar las argumentaciones vertidas de mi parte.
- Que una vez evaluadas las argumentaciones y pruebas de descargo, se tenga por DESVANECIDOS los hallazgos relacionados, por las razones ya argumentadas de mi parte.
- Que se sirvan notificarme el desvanecimiento de los referidos hallazgos”.

Mediante oficio s/n de fecha 16 de enero de 2019, la señora Brenda Amarilis Gramajo González, Director Ejecutivo del Registro Nacional de las Personas, durante el período del 02 de junio al 31 de septiembre de 2016, expone lo siguiente: “Sobre la responsabilidad en cuanto a tomar acciones en relación a la administración y manejo de un sistema de nóminas en el Registro Nacional de las Personas, corresponde directamente a la Dirección Administrativa y a la Subdirección de Recursos Humanos, según lo establecido en el Acuerdo de Directorio número 80-2016, para lo cual me permito citar los artículos siguientes:

“Artículo 61. Dirección Administrativa. Es la dependencia que tiene a su cargo organizar y ejecutar las actividades administrativas de la Institución. Propone al



Directorio del RENAP, por medio del Director Ejecutivo, la política en la administración de los recursos humanos, financieros...”.

La literal a) del mismo artículo establece: “a) Proponer e implementar políticas, normativas, estrategias, procesos y procedimientos en materia administrativa y de recursos humanos”.

“Artículo 68. Subdirección de Recursos Humanos. Es la dependencia encargada de los procesos administrativos de puestos, reclutamiento, selección, gestión de personal, evaluación del desempeño, seguridad e higiene laboral, sueldos y salarios, de conformidad con las políticas, lineamientos y disposiciones legales en materia de recursos humanos.”

“Artículo 69. Departamento de Reclutamiento y Selección. Es la dependencia encargada de la planificación, organización, ejecución y coordinación de todas las acciones encaminadas al reclutamiento y selección de personal idóneo tanto interno como externo, con la finalidad de cubrir las necesidades de personal de la institución, así como, efectuar procesos relacionados con la administración de puestos”.

“Artículo 71. Departamento de Nóminas. Es la dependencia encargada de procesar la información del recuso humano que trabaja en la Institución, para realizar los pagos y deducciones correspondientes; a fin de que sus retribuciones les sean pagadas oportunamente, entiendo y forma, con base a los lineamientos de las leyes, decretos, reglamentos, acuerdos y otros establecidos así como realizar otros estudios relacionados con la administración de salarios.”

Por lo expuesto, a través de la normativa legal citada, que tomó vigencia durante el período en que fungí como Director Ejecutivo en Funciones del RENAP, se delimitó la responsabilidad de la Dirección Administrativa y la Subdirección de Recursos Humanos; en ese sentido la responsabilidad directa de la administración así como de la implementación de los diferentes tipos de control que se relacionan con los sistemas administrativos financieros en materia de recursos humanos, quedó con claridad bajo la responsabilidad de la Subdirección de Recursos Humanos del RENAP.

Bajo estos criterios, por medio de oficio número Ref. oficio DA-0793-2016 de fecha 26 de mayo de 2016, se hace referencia al oficio DE-1524-2016 por medio del cual se giran instrucciones a la Subdirección de Recursos Humanos del RENAP, darle seguimiento a la implementación del sistema GUATENOMINAS, en el Registro Nacional de las Personas, por lo que la ejecución a dicha instrucción corresponde a la Subdirección de Recursos Humanos”.





Comentario de la Auditoría

Se confirma el presente hallazgo para el señor Rony Domingo Ibáñez Ramírez, quién fungió como Jefe de Nóminas del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de enero de 2015 al 31 de octubre de 2016, en virtud que no obstante a partir del año dos mil catorce realizó gestiones para la implementación del "Sistema Informático de RH/Nóminas Delta" y del Sistema de Nóminas y Registro de Personal Guatenóminas, durante el período de la auditoría persistía la elaboración de las nóminas a través de Microsoft Excel, lo que representa vulnerabilidad de los datos, riesgo de la seguridad e integridad de la información.

Se confirma el presente hallazgo para la señora Telma Mirella Lorenzana Noriega, quién fungió como Director Administrativo del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de enero de 2015 al 30 de junio de 2016, en virtud que no se presentó a la discusión de hallazgos y tampoco presentó las pruebas de descargo.

Se confirma el presente hallazgo para el señor Eduardo Salvador Navarro Molina, quién fungió como Director Administrativo del Registro Nacional de las Personas -RENAP- por el período comprendido del 16 de mayo al 21 de septiembre de 2016 en virtud que no obstante a que realizó gestiones para la implementación del Sistema de Nóminas y Registro de Personal Guatenóminas, durante el período de la auditoría persistía la elaboración de las nóminas a través de Microsoft Excel, lo que representa vulnerabilidad de los datos, riesgo de la seguridad e integridad de la información.

Se confirma el presente hallazgo para el señor Rudy Leonel Gallardo Rosales, quién fungió como Director Ejecutivo del Registro Nacional de las Personas -RENAP- por el período comprendido del 01 de enero de 2015 al 01 de junio de 2016, en virtud que no obstante a las gestiones e instrucciones emitidas por la Dirección Ejecutiva sobre la implementación del Sistema de Nóminas y Registro de Personal Guatenóminas, durante el período de la auditoría las nóminas se elaboran a través de Microsoft Excel, lo cual representa vulnerabilidad de los datos, riesgo de la seguridad e integridad de la información.

Se confirma el presente hallazgo para el señora Brenda Amarilis Gramajo González, quién fungió como Director Ejecutivo del Registro Nacional de las Personas -RENAP- por el período comprendido del 02 de junio al 31 de octubre de 2016, en virtud que no obstante a que la función de nóminas corresponde a otra unidad administrativa se elaboran a través de Microsoft Excel, lo cual representa vulnerabilidad de los datos, riesgo de la seguridad e integridad de la información.

Este hallazgo fue notificado con el número 11 y corresponde en el presente





informe al número 7.

Acciones Legales y Administrativas

Sanción económica de conformidad con el Decreto 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, reformada por el Decreto 13-2013; artículo 39, Numeral 4, para:

Cargo	Nombre	Valor en Quetzales
DIRECTOR EJECUTIVO	RUDY LEONEL GALLARDO ROSALES	12,000.00
DIRECTOR EJECUTIVO	BRENDA AMARILIS GRAMAJO GONZALEZ	12,000.00
DIRECTOR ADMINISTRATIVO	TELMA MIRELLA LORENZANA NORIEGA	7,500.00
DIRECTOR ADMINISTRATIVO	EDUARDO SALVADOR NAVARRO MOLINA	7,500.00
JEFE DE NOMINAS	RONY DOMINGO IBAÑEZ RAMIREZ	4,500.00
Total		Q. 43,500.00





7. AUTORIDADES DE LA ENTIDAD, DURANTE EL PERÍODO AUDITADO

Los funcionarios y empleados responsables de las deficiencias encontradas, se incluyen en el desarrollo de cada hallazgo contenido en el presente informe.

No.	NOMBRE	CARGO	PERÍODO
1	RUDY LEONEL GALLARDO ROSALES	DIRECTOR EJECUTIVO	01/01/2015 - 01/06/2016
2	BRENDA AMARILIS GRAMAJO GONZALEZ	DIRECTOR EJECUTIVO	02/06/2016 - 31/10/2016
3	TELMA MIRELLA LORENZANA NORIEGA	DIRECTOR ADMINISTRATIVO	01/01/2015 - 30/06/2016
4	EDUARDO SALVADOR NAVARRO MOLINA	DIRECTOR ADMINISTRATIVO	22/09/2016 - 31/10/2016
5	CARLOS ALBERTO QUINTANA GALINDO	DIRECTOR DE INFORMATICA Y ESTADISTICA	01/01/2015 - 31/10/2016
6	GUILLERMO (S.O.N) BRINCKER SOCORRO	DIRECTOR DE PROCESOS	01/01/2015 - 31/03/2015
7	MONICA RENEE RECINOS CASANOVA	DIRECTOR DE PROCESOS	06/04/2015 - 01/07/2015
8	BRENDA AMARILIS GRAMAJO GONZALEZ	DIRECTOR DE PROCESOS	08/10/2015 - 31/10/2016

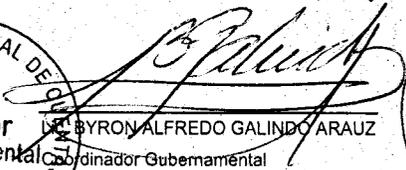


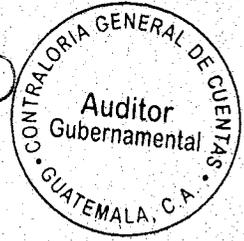


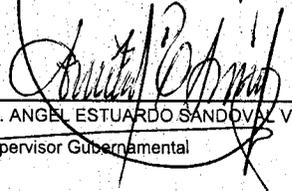
8. COMISIÓN DE AUDITORÍA ÁREA TÉCNICA


Ing. ERICKSON ALEXANDER AQUECHE PADILLA
Auditor Gubernamental




Lic. BYRON ALFREDO GALINDO ARAUZ
Coordinador Gubernamental



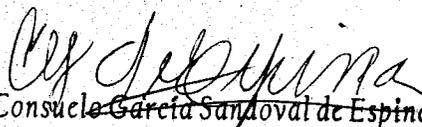

Lic. ANGEL ESTUARDO SANDOVAL VILLATORO
Supervisor Gubernamental



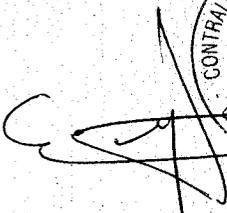
RAZÓN:

De conformidad con lo establecido en el Decreto No. 31-2002, del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, artículo 29, los auditores gubernamentales nombrados son responsables del contenido y efectos legales del presente informe, el Director y Subdirector únicamente firman en constancia de haber conocido el contenido del mismo.

INFORME CONOCIDO POR:


Licda. Consuelo García Sandoval de Espina
Subdirectora de Auditoría a Sistemas Informáticos y
Nóminas de Gobierno




Licda. Emma Gabriela Luna López
Directora de Auditoría a Sistemas
Informáticos y Nóminas de Gobierno





ANEXOS







Contraloría General de Cuentas

GUATEMALA, C.A.

DIRECCIÓN DE AUDITORÍA A SISTEMAS INFORMÁTICOS Y NOMINAS DE GOBIERNO NOMBAMIENTO DE AUDITORÍA INFORMÁTICA



CUA: 55291

DAS-12-0009-2017

Guatemala, 18 de mayo de 2017

Auditor(es) Gubernamental(es):

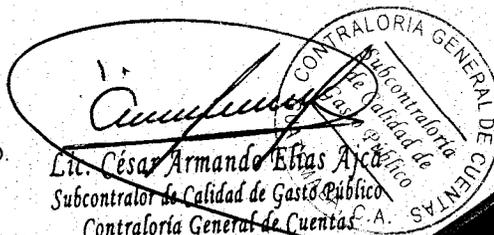
LIC. BYRON ALFREDO GALINDO ARAUZ, COORDINADOR
ING. ERICKSON ALEXANDER AQUECHE PADILLA, AUDITOR
LIC. ANGEL ESTUARDO SANDOVAL VILLATORO, SUPERVISOR

Respetuosamente me dirijo a ustedes, para hacer de su conocimiento que, en sustitucion al nombramiento DASI-0076-2016 y la modificación efectuada, según nombramiento DASI-0016-2017, en cumplimiento a los artículos 232 de la Constitución Política de la República de Guatemala; artículos 2 y 7 del Decreto Número 31-2002 del Congreso de la República de Guatemala, Ley Orgánica de la Contraloría General de Cuentas y sus reformas; artículos 57, 68 y 75 del Acuerdo Gubernativo Número 9-2017, Reglamento de la Ley Orgánica de la Contraloría General de Cuentas, esta Dirección los designa; para que en representación de esta Institución, se presenten al REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, CON LA CUENTA No. R1-60, para practicar Auditoría de Sistemas Informáticos.

En la práctica de auditoría, deberán determinar el cumplimiento de la legalidad vigente a las que está sujeto, la eficiencia y la eficacia de los procesos soportados por el sistema en cuestión, en especial los de la administración electrónica y todos los aspectos inherentes que considera necesarios, el periodo a fiscalizar es del 01/01/2015 al 31/10/2016. Para el cumplimiento de lo anterior, deberá observar las Normas de Auditoría del Sector Gubernamental, Normas de Control Interno Gubernamental, así como Leyes y disposiciones vigentes aplicables a la Entidad auditada, para lo cual se recomienda verificar lo siguiente: Planificación y Organización de las TI, Recursos Humanos para TI, Infraestructura en TI, Seguridad de la Información, Recomendaciones de la auditoría anterior y Grupo de Gasto 100 y 300, renglones 158, 328 y 381, así como todo el proceso de la emisión del Documento Personal de Identificación y el cumplimiento de regulaciones legales. Así mismo, se hace de su conocimiento que la comisión nombrada anteriormente, hará entrega de un informe circunstanciado de las actuaciones que han realizado a la fecha, con el cual dieron cumplimiento al nombramiento DASI-0076-2016.

Los resultados de sus actuaciones los harán constar en actas circunstanciadas que se suscriban y papeles de trabajo que elaboren para el efecto, tomando y/o dictando las medidas de orden técnico e Informático y haciendo cumplir las Leyes vigentes que procedan, formulando las observaciones y recomendaciones en el informe pertinente. Dicho informe deberán presentarlo a esta Dirección oportunamente. El tiempo estimado para realizar esta Auditoría Informática es de 20 días, el cual puede variar según las circunstancias que se presenten en el desarrollo del trabajo.

Inga. Emma Guariela López
Directora de Auditoría a Sistemas
Informáticos y Nóminas de Gobierno



Este nombramiento puede ser consultado en la página web. (<http://www.contraloria.gob.gt>)





Contraloría General de Cuentas

GUATEMALA, C.A.

**DIRECCIÓN DE AUDITORÍA DE SISTEMAS INFORMÁTICOS
NOMBRAMIENTO DE AUDITORÍA INFORMÁTICA**



**CUA: 53915
DASI-0076-2016**

Guatemala, 28 de octubre de 2016

Auditor(es) Gubernamental(es):

INGA. MARIELA EDITH MERIDA RODRIGUEZ, AUDITORA
LIC. MANUEL RAUL SOSA IPIÑA, COORDINADOR
LICDA. SANDRA ANABELLA TOBAR PARADA, SUPERVISORA

Respetuosamente me dirijo a ustedes, para hacer de su conocimiento que, con fundamento en los artículos 2 y 7 del Decreto Número 31-2002 del Congreso de la República de Guatemala, Ley Orgánica de la Contraloría General de Cuentas y sus reformas; artículo 2 incisos l y n; artículos 5 y 51 del Acuerdo Gubernativo Número 192-2014, Reglamento de la Ley Orgánica de la Contraloría General de Cuentas y norma 3.4 de las Normas de Auditoría del Sector Gubernamental; se les designa, para que en representación de esta Institución, se presenten al REGISTRO NACIONAL DE LAS PERSONAS -RENAP- CON LA CUENTA No. R1-60, para practicar Auditoría de Sistemas Informáticos.

Determinar el cumplimiento de la legalidad vigente a las que está sujeto, la eficiencia y la eficacia de los procesos soportados por el sistema en cuestión, en especial los de la administración electrónica y todos los aspectos inherentes que considera necesarios, el período a fiscalizar es del 01/01/2015 al 31/10/2016. Para el cumplimiento de lo anterior, deberá observar las Normas de Auditoría del Sector Gubernamental, Normas de Control Interno Gubernamental, así como Leyes y disposiciones vigentes aplicables a la Entidad auditada, para lo cual se recomienda verificar lo siguiente: Planificación y Organización de las TI, Recursos Humanos para TI, Infraestructura en TI, Seguridad de la Información, Recomendaciones de la auditoría anterior y Grupo de Gasto 100 y 300, renglones 158, 328 y 381 y el cumplimiento de regulaciones legales.

Los resultados de sus actuaciones los harán constar en actas circunstanciadas que se suscriban y papeles de trabajo que elaboren para el efecto, tomando y/o dictando las medidas de orden técnico e Informático y haciendo cumplir las Leyes vigentes que procedan, formulando las observaciones y recomendaciones en el informe pertinente. Dicho informe deberán presentarlo a esta Unidad oportunamente.

El tiempo estimado para realizar esta Auditoría Informática es de 20 días, el cual puede variar según las circunstancias que se presenten en el desarrollo del trabajo.



Inga. Emma Gabriela Luna López.
Directora de Auditoría de Sistemas Informáticos
Contraloría General de Cuentas

Vo.Bo.:

César Armando Elías Arce
Contraloría General de Cuentas

Este nombramiento puede ser consultado en la página web. (<http://www.contraloria.gob.gt>)





Contraloría General de Cuentas
GUATEMALA, C.A.

DECLARACIÓN ESPECÍFICA DE INDEPENDENCIA

Yo : ANGEL ESTUARDO SANDOVAL VILLATORO en mi calidad de SUPERVISOR GUBERNAMENTAL de la DIRECCION DE AUDITORIAS A SISTEMAS INFORMATICOS Y NOMINAS DE GOBIERNO. Declaro que he sido nombrado para realizar auditoria en: REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, según nombramiento DAS-12-0009-2017, de fecha 18/05/2017, en donde a mi leal saber y entender, no tengo intereses personales, comerciales, financieros o económicos directos o indirectos; ni conflictos de interés de cualquier índole, tampoco tengo compromiso de servicios, trabajos o dependencia con dicha entidad.

Declaro que ningún miembro de mi familia en los grados de ley, desempeña cargo de autoridad superior ni tiene relación directa en el desempeño de mi trabajo como auditor gubernamental, en la entidad descrita anteriormente.

Me comprometo a informar oportunamente y por escrito cualquier impedimento o conflicto de interés de tipo personal, profesional o contractual, sobreviniente a esta declaración, los que pueden ser: inhabilitación profesional, amistad íntima, enemistad, odio o resentimiento, litigios pendientes, razones religiosas, políticas e ideológicas u otras que afecten mi independencia.

En el ejercicio de mis funciones como SUPERVISOR GUBERNAMENTAL es posible que tenga acceso a información sobre distintos aspectos de la entidad auditada y otras relaciones que, por lo general no están disponibles al público. Comprendo plenamente que poseer esta información requiere el más alto nivel de integridad y confidencialidad, comprometiendome a no divulgarla ni utilizarla sin la debida autorización.

Hago constar que en todo momento me conduciré con responsabilidad, honestidad y profesionalismo en el desarrollo de mis actos y no utilizaré la investidura que me otorgan, para requerir favores, beneficios personales o a favor de terceros; tampoco a grupos a los que pertenezca.

Nota: Los datos que se consignen en la presente deberán ser verdaderos, caso contrario se deducirán las responsabilidades legales y administrativas correspondientes.

Lugar y Fecha Guatemala, 18 de Mayo de 2017

f)

SUPERVISOR GUBERNAMENTAL





Contraloría General de Cuentas
GUATEMALA, C.A.

DECLARACIÓN ESPECÍFICA DE INDEPENDENCIA

Yo : BYRON ALFREDO GALINDO ARAUZ en mi calidad de AUDITOR INDEPENDIENTE de la DIRECCION DE AUDITORIAS A SISTEMAS INFORMATICOS Y NOMINAS DE GOBIERNO. Declaro que he sido nombrado para realizar auditoria en: REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, según nombramiento DAS-12-0009-2017, de fecha 18/05/2017, en donde a mi leal saber y entender, no tengo intereses personales, comerciales, financieros o económicos directos o indirectos; ni conflictos de interés de cualquier índole, tampoco tengo compromiso de servicios, trabajos o dependencia con dicha entidad.

Declaro que ningún miembro de mi familia en los grados de ley, desempeña cargo de autoridad superior ni tiene relación directa en el desempeño de mi trabajo como auditor gubernamental, en la entidad descrita anteriormente.

Me comprometo a informar oportunamente y por escrito cualquier impedimento o conflicto de interés de tipo personal, profesional o contractual, sobreviniente a esta declaración, los que pueden ser: inhabilitación profesional, amistad íntima, enemistad, odio o resentimiento, litigios pendientes, razones religiosas, políticas e ideológicas u otras que afecten mi independencia.

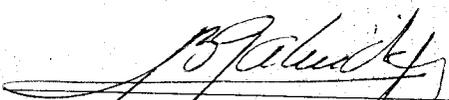
En el ejercicio de mis funciones como AUDITOR INDEPENDIENTE es posible que tenga acceso a información sobre distintos aspectos de la entidad auditada y otras relaciones que, por lo general no están disponibles al público. Comprendo plenamente que poseer esta información requiere el más alto nivel de integridad y confidencialidad, comprometiendome a no divulgarla ni utilizarla sin la debida autorización.

Hago constar que en todo momento me conduciré con responsabilidad, honestidad y profesionalismo en el desarrollo de mis actos y no utilizaré la investidura que me otorgan, para requerir favores, beneficios personales o a favor de terceros; tampoco a grupos a los que pertenezca.

Nota: Los datos que se consignan en la presente deberán ser verdaderos, caso contrario se deducirán las responsabilidades legales y administrativas correspondientes.

Lugar y Fecha Guatemala, 18 de Mayo de 2017

f)



AUDITOR INDEPENDIENTE





Contraloría General de Cuentas
GUATEMALA, C.A.

DECLARACIÓN ESPECÍFICA DE INDEPENDENCIA

Yo : ERICKSON ALEXANDER AQUECHE PADILLA en mi calidad de AUDITOR INDEPENDIENTE de la DIRECCION DE AUDITORIAS A SISTEMAS INFORMATICOS Y NOMINAS DE GOBIERNO. Declaro que he sido nombrado para realizar auditoria en: REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, según nombramiento DAS-12-0009-2017, de fecha 18/05/2017, en donde a mi leal saber y entender, no tengo intereses personales, comerciales, financieros o económicos directos o indirectos; ni conflictos de interés de cualquier índole, tampoco tengo compromiso de servicios, trabajos o dependencia con dicha entidad.

Declaro que ningún miembro de mi familia en los grados de ley, desempeña cargo de autoridad superior ni tiene relación directa en el desempeño de mi trabajo como auditor gubernamental, en la entidad descrita anteriormente.

Me comprometo a informar oportunamente y por escrito cualquier impedimento o conflicto de interés de tipo personal, profesional o contractual, sobreviniente a esta declaración, los que pueden ser: inhabilitación profesional, amistad íntima, enemistad, odio o resentimiento, litigios pendientes, razones religiosas, políticas e ideológicas u otras que afecten mi independencia.

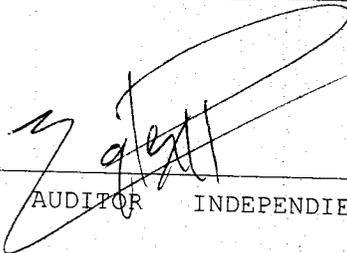
En el ejercicio de mis funciones como AUDITOR INDEPENDIENTE es posible que tenga acceso a información sobre distintos aspectos de la entidad auditada y otras relaciones que, por lo general no están disponibles al público. Comprendo plenamente que poseer esta información requiere el más alto nivel de integridad y confidencialidad, comprometiendome a no divulgarla ni utilizarla sin la debida autorización.

Hago constar que en todo momento me conduciré con responsabilidad, honestidad y profesionalismo en el desarrollo de mis actos y no utilizaré la investidura que me otorgan, para requerir favores, beneficios personales o a favor de terceros; tampoco a grupos a los que pertenezca.

Nota: Los datos que se consignen en la presente deberán ser verdaderos, caso contrario se deducirán las responsabilidades legales y administrativas correspondientes.

Lugar y Fecha Guatemala, 18 de Mayo de 2017

f)



AUDITOR INDEPENDIENTE

FORMA ÚNICA DE ESTADÍSTICA

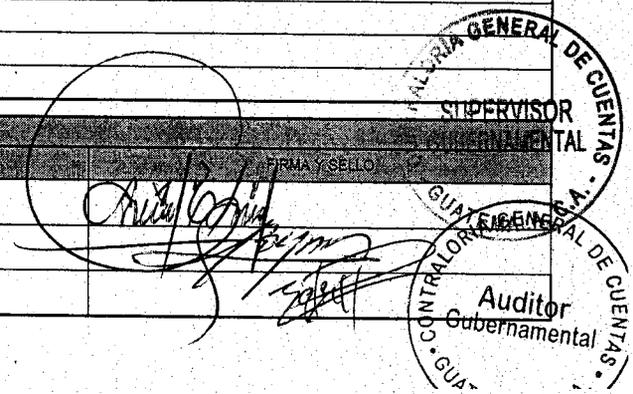
1 DATOS GENERALES			
1.1 ORGANIZACIÓN, ENTIDAD, INSTITUCIÓN, O FIDEICOMIS	Registro Nacional de Las Personas		
1.2 ENTIDAD A LA QUE PERTENCE:	Registro Nacional de Las Personas		
1.3 TIPO DE ENTIDAD	Administración central (Gobierno) <input checked="" type="checkbox"/>	Descentralizada <input type="checkbox"/>	Autónoma <input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Municipalidades <input type="checkbox"/>		Entidades Especiales <input type="checkbox"/>
1.4 NÚMERO DE CUENTADANCIA O REGISTRO	R1-60		
1.5 DIRECCIÓN QUE EMITE EL NOMBRAMIENTO	AUDITORÍA A SISTEMAS INFORMÁTICOS Y NÓMINAS DE GOBIERNO		
1.6 NOMBRAMIENTO N.º (S)	DAS-12-0009-2017		
1.7 FECHA EMISIÓN DE NOMBRAMIENTO(S)	19 de mayo de 2017		FIRMA Y SELLO DE ESTADÍSTICA - UNIDAD DE PLANIFICACIÓN
1.8 AUDITOR(ES), GUBERNAMENTAL(ES) ASIGNADOS	Lic. Byron Alfredo Galindo Arauz, Ing. Erickson Alexander Aqueche Padilla y Lic. Angel Estuardo Sandoval Villatoro		
1.9 CODIGO (Exclusivo estadística)			
1.10 PERIODO AUDITADO	DEL	Día Mes Año 1 1 2015	AL
		Día Mes Año 31 10 2016	No. MESES AUDITADOS 22

2 AUDITORIA				5 OBRA PÚBLICA			
2.1 TIPO DE AUDITORIA O COMISIÓN		AUDITORÍA A SISTEMAS INFORMATICOS		TIPO DE OBRA		*No.Obras	
2.2 TOTAL MONTO AUDITADO		Q -		Puentes	Q	Monto	
Saldo anterior*		Q -		Pavimentos	Q		
Ingresos		Q -		Edificios Escolares	Q		
Egresos		Q -		Otros edificios	Q		
*Ingresar únicamente si es examen especial				Salón usos múltiples	Q		
				Const. Y Mant. Carretera	Q		
				Instalaciones Deportivas	Q		
				Sistema de Agua Potable	Q		
				Drenajes	Q		
				Energía Eléctrica	Q		
				Otros			
				TOTAL	0	Q	
				*Si es más de una obra agregar anexo			

3 ACCIONES LEGALES Y ADMINISTRATIVAS				
3.1 *SANCIÓN				
Cantidad	Tipo de hallazgo		Monto en Q.	Fundamento Legal
	CI	C		
7	X		Q 181,000.00	Decreto 31-2002 del Congreso de la República, Ley Organica de la Contraloría General de Cuentas, Artículo 39.
3.2 *FORMULACIÓN DE CARGO				
Cantidad	Tipo de hallazgo		Monto en Q.	Fundamento Legal
	CI	C		
3.3 *DENUNCIA				
Cantidad	Tipo de hallazgo		Monto en Q.	Fundamento Legal
	CI	C		
*Si es más de UNA Sanción, Formulación de cargos o Denuncia, agregar anexo -				

4 PRESUPUESTO			
Presupuesto Asignado			
Modificaciones (+) ó (-)		Q -	
Vigente		Q -	
Ejecutado		Q -	
Por devengar		Q -	

7 NOMBRE, CARGO, FIRMA Y SELLO DE SUPERVISOR, COORDINADOR Y AUDITORES RESPONSABLES			
NOMBRES		CARGO	
Lic. Angel Estuardo Sandoval Villatoro		Supervisor	
Lic. Byron Alfredo Galindo Arauz		Coordinador	
Ing. Erickson Alexander Aqueche Padilla		Auditor	



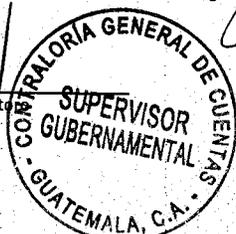
FORMA UNICA DE ESTADÍSTICA
ANEXO DEL NUMERAL 3.1

No.	Hallazgo No. 1 Vulnerabilidad en la seguridad de los servicios de la red interna	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	MANUEL ALEJANDRO RIMOLA CORDERO		X	Q 4,500.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	CARLOS ALBERTO QUINTANA GALINDO		X	Q 7,500.00			
3	OMAR ESDUARDO SAGASTUME ALVAREZ		X	Q 4,500.00			
4	MONICA CAROLINA CARCAMO RECINOS		X	Q 4,500.00		Q 21,000.00	
No.	Hallazgo No. 2 Falta de procedimientos para el uso de bitácoras	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	PAUL ENRIQUE HERNANDEZ CIFUENTES		X	Q 4,500.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	LAI YEE LEUNG NG		X	Q 4,500.00			
3	DANY JOSUE MINCHEZ MONZON		X	Q 4,500.00		Q 13,500.00	
No.	Hallazgo No. 3 Desactualización de los Parches en la base de Datos	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	PAUL ENRIQUE HERNANDEZ CIFUENTES		X	Q 4,500.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	LAI YEE LEUNG NG		X	Q 4,500.00			
3	DANY JOSUE MINCHEZ MONZON		X	Q 4,500.00		Q 13,500.00	
No.	Hallazgo No. 4 Falta de un Plan de Continuidad del Negocio -BCP-	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	RUDY LEONEL GALLARDO ROSALES		X	Q 12,000.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	BRENDA AMARILIS GRAMAJO GONZALEZ		X	Q 12,000.00			
3	CARLOS ALBERTO QUINTANA GALINDO		X	Q 7,500.00			
4	HECTOR IVAN GARCIA SOLORZANO		X	Q 5,750.00			
5	EDUARDO SALVADOR NAVARRO MOLINA		X	Q 5,750.00		Q 43,000.00	
No.	Hallazgo No. 5 Falta de un Oficial de Seguridad	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	CARLOS ALBERTO QUINTANA GALINDO		X	Q 7,500.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	HECTOR IVAN GARCIA SOLORZANO		X	Q 5,750.00			
3	EDUARDO SALVADOR NAVARRO MOLINA		X	Q 5,750.00		Q 19,000.00	
No.	Hallazgo No. 6 Falta de seguridad y condiciones apropiadas en el área de trabajo	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	TELMA MIRELLA LORENZANA NORIEGA		X	Q 7,500.00		Q 7,500.00	El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
No.	Hallazgo No. 6 Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos	TIPO DE HALLAZGO		MONTO	RESPONSABLES	MONTO TOTAL SANCION	FUNDAMENTO LEGAL
		CUMPLIMIENTO	CONTROL INTERNO				
1	RUDY LEONEL GALLARDO ROSALES		X	Q 12,000.00			El Decreto No.31-2002, Ley Orgánica de la C. G. C., artículo 39, numeral 4.
2	BRENDA AMARILIS GRAMAJO GONZALEZ			Q 12,000.00			
3	TELMA MIRELLA LORENZANA NORIEGA			Q 7,500.00			
4	EDUARDO SALVADOR NAVARRO MOLINA			Q 7,500.00			
5	RONY DOMINGO IBAÑEZ RAMIREZ			Q 4,500.00		Q 43,500.00	
Total				7	Q 80,000.00	Q 161,000.00	

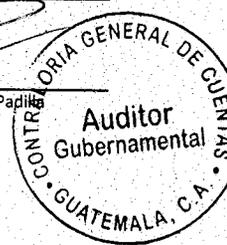
Lic. Byron Alfredo Gatindo Arauz
Auditor Gubernamental



Lic. Ángel Estuardo Sandoval Viqueo
Supervisor Gubernamental



Ing. Erickson Alexander Aqueche Padilla
Auditor Gubernamental







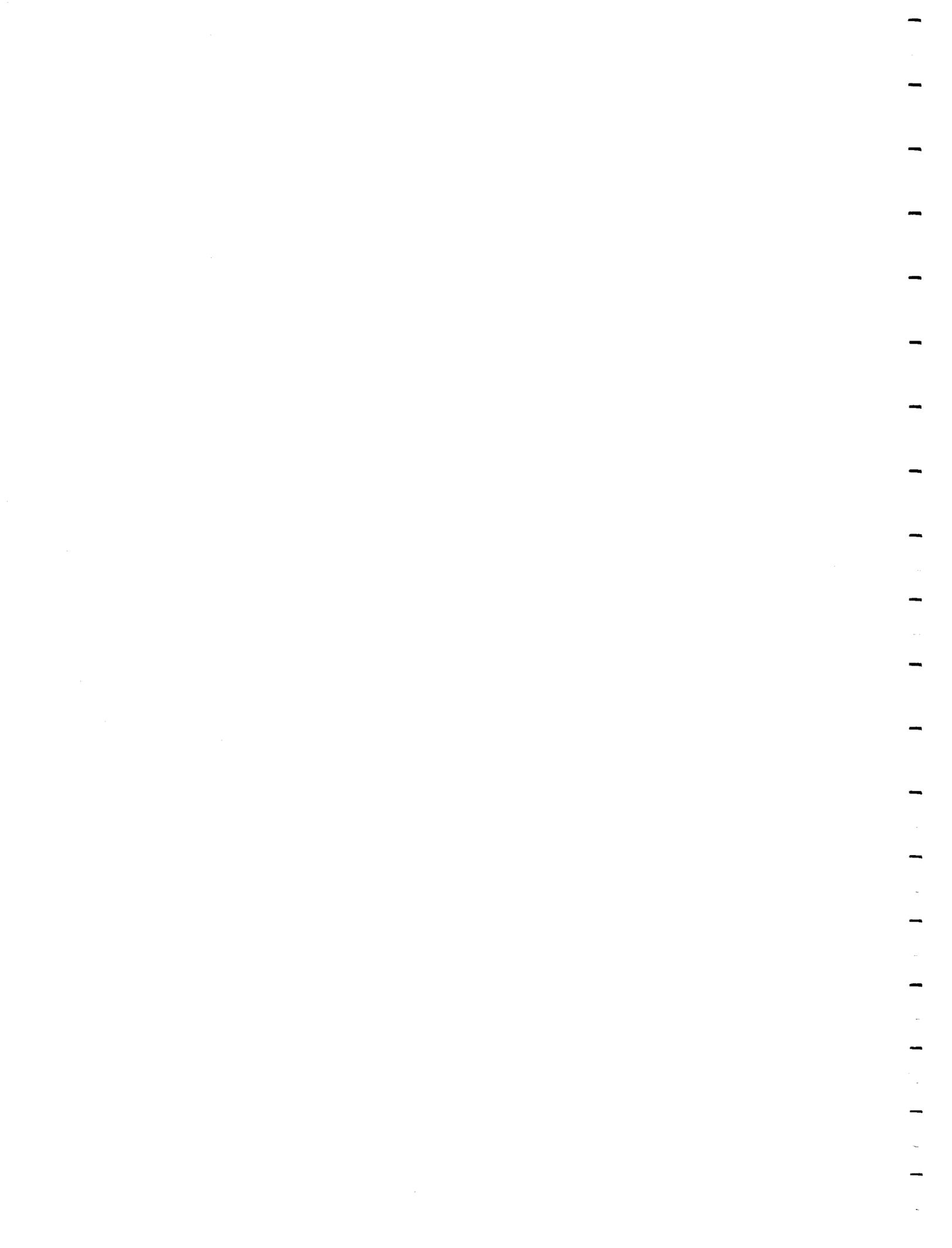
<p>Vulnerabilidad a ataques DoS y uso de imagen para Phishing</p> <ol style="list-style-type: none"> Se determinó que no se cuenta con herramientas que monitoreen y garanticen que el Portal Web siempre se encuentre disponible lo que origina que sea vulnerable a ataques de denegación de servicios (DoS). Se observó que el código HTML y Scripts, de los componentes utilizados dentro del Portal Web puede ser visualizado con facilidad, dándole click derecho sobre él, originando que pueda ser utilizado por un hacker para realizar phishing, con la imagen de la institución. <p>No se aplica Protocolos de seguridad HTTPS, en los Formularios de solicitud de información del portal web.</p> <p>No se aplica Protocolos de seguridad HTTPS, en los Formularios de solicitud de información del portal web.</p>									
<p>Recomendación:</p> <p>El Director Ejecutivo debe girar sus instrucciones al Director de Informática y Estadística y este a su vez al Jefe y técnico encargado de la seguridad en el Departamento de Seguridad Informática, para que se efectúen las acciones necesarias para garantizar que las impresoras no queden inhabilitadas, la imagen institucional, la información administrada por los formularios del portal web sean utilizadas por terceras personas, así como la disponibilidad de dicho Portal.</p>									
<p>HALLAZGO No. 2</p> <p>Falta de procedimientos para el uso de bitácoras</p>									
<p>Condición:</p> <p>En el Registro Nacional de las Personas - RENAP, se observó que actualmente tiene acceso el Administrador de la Base de Datos</p>									

- PAUL ENRIQUE HERNANDEZ CIFUENTES
- LAI YEE LEUNG NG
- DANY JOSUE MINCHEZ MONZON

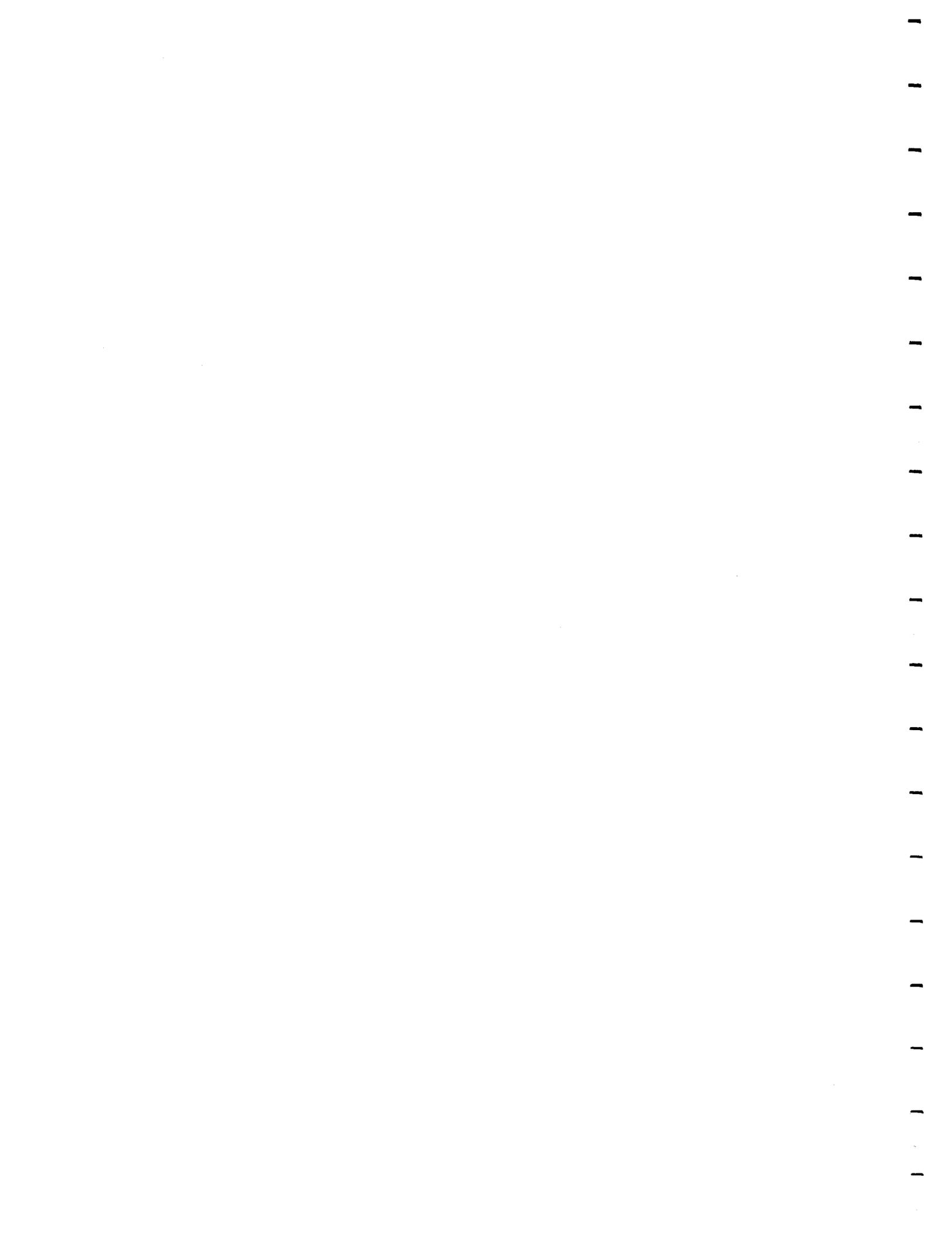


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

	sistema gestor de Base de Datos, como una medida preventiva para mitigar los riesgos en el sistema que podrían surgir por no realizarlas actualizaciones. HALLAZGO No. 4									
	Falta de un Plan de Continuidad del Negocio -BCP-	<ul style="list-style-type: none"> • RUDY LEONEL GALLARDO ROSALES • BRENDA AMARILIS GRAMAJO GONZALEZ • CARLOS ALBERTO QUINTANA GALINDO • HECTOR IVAN GARCIA SOLORZANO • EDUARDO SALVADOR NAVARRO MOLINA 								
	Condición: En el Departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, se determinó al efectuar la auditoría a sistemas informáticos que no cuentan con un Plan de Continuidad del Negocio, (Business Continuity Planning -BCP-), a nivel de tecnología de la información, aprobado por la Dirección Ejecutiva en donde se detalle las actividades en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección Informática y Estadística.									
	Recomendación: El Directorio del Registro Nacional de las Personas debe girar instrucciones al Director Ejecutivo, Director de Informática y Estadística, Subdirector de Sistemas y Estadística y Subdirector de Servicios Críticos, para que se elabore un plan de continuidad del negocio, en donde se establezcan los procedimientos internos a realizar y se especifique a los responsables en caso de alguna contingencia que tenga que ver con los servicios críticos que proporciona la Dirección Informática y Estadística.									
	HALLAZGO NO. 5									
	Falta de Un Oficial de Seguridad	<ul style="list-style-type: none"> • CARLOS ALBERTO QUINTANA GALINDO • HECTOR IVAN GARCIA SOLORZANO • EDUARDO SALVADOR NAVARRO MOLINA 								



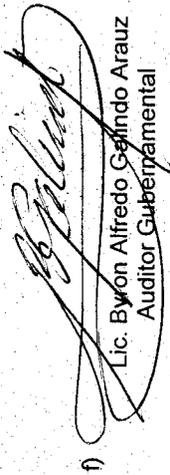
	<p>Condición: En el Registro Nacional de las Personas - RENAP-, se observó dentro del Organigrama Institucional del RENAP, que no se tiene implementada la figura de un Oficial de Seguridad Informático (OSI), que tenga a su cargo las funciones de prevención, análisis y detección de vulnerabilidades en materia de seguridad informática.</p>					
	<p>Recomendación: El Director Ejecutivo, debe girar sus instrucciones al Director de Informática y Estadística y al Subdirector de Servicios Críticos para crear un procedimiento, en el cual un experto en seguridad ajeno al Departamento de Informática y Estadística, realice las evaluaciones necesarias para mitigar las posibles vulnerabilidades informáticas en la infraestructura de red y sistemas utilizadas por el Registro Nacional de Las Personas.</p>					
	<p>HALLAZGO No. 6</p>					
	<p>Falta de seguridad y condiciones apropiadas en el área de trabajo</p>	<ul style="list-style-type: none"> • TELMA MIRELLA LORENZANA NORIEGA 				
	<p>Condición: En el Registro Nacional de las Personas - RENAP-, la comisión de auditoría a sistemas informáticos, determinó que no se cuenta con las medidas de seguridad mínimas en el ingreso al área restringida del Departamento de Control de Calidad, en donde se resguardan físicamente los DPI personalizados, las cuales se describen a continuación:</p> <ol style="list-style-type: none"> 1. No se cuenta con una puerta que aisle la unidad catalogada como área restringida. 2. No cuenta con el sistema de cámaras de circuito cerrado de televisión-CCTV-. 3. Carecen de extintores en el área y existe material inflamable como cajas de cartón, cajas y bolsas plásticas de empaque para los DPI. 4. No se cuenta con una caja de seguridad, en donde se resguarden documentos de valor, como serían los DPI impresos. 					



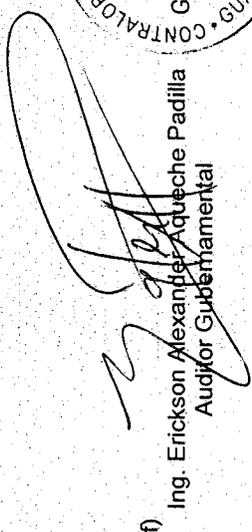
	<p>Recomendación: El Directorio debe girar sus instrucciones al El Director Ejecutivo, al Director y Sub Director de Procesos y al Director Administrativo, para crear las condiciones necesarias de seguridad para mantener el área restringida donde se localizan los Documentos de Identificación Personal ya emitidos, para su revisión por parte del Departamento de Control de Calidad.</p>						
	<p>HALLAZGO No. 7 Falta de Sistema de Nóminas para Administrar la Gestión de Recursos Humanos</p>	<ul style="list-style-type: none"> • RUDY LEONEL GALLARDO ROSALES • BRENDA AMARILIS GRAMAJO GONZALEZ • TELMA MIRELLA LORENZANA NORIEGA • EDUARDO SALVADOR NAVARRO MOLINA • RONY DOMINGO IBANEZ RAMIREZ 					
	<p>Condición: En el departamento de Análisis de Sistemas de Información del Registro Nacional de las Personas -RENAP-, se observó que no existe un sistema de nóminas del personal y que durante los 10 años que tiene el RENAP de estar funcionando, la nómina de empleados que asciende a 2,256 empleados, se registra en hojas de cálculo Excel.</p>						
	<p>Recomendación: El Director Ejecutivo, Director Administrativo, Subdirector de Recursos Humanos y este a su vez al Jefe del Departamento de Nóminas, para que soliciten al Jefe del Departamento de Análisis de Sistemas de Información que realice el análisis y desarrollo de un sistema de nóminas, en tanto no adopten el Sistema Guatenóminas.</p>						

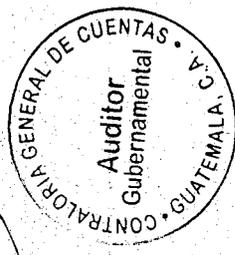


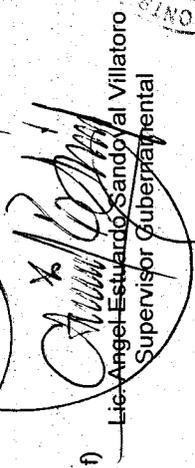
NOTA: Auditoria a Sistemas Informáticos al Registro Nacional de las Personas -RENAP-, determinando el cumplimiento de la legalidad vigente a las que está sujeto, la eficiencia y la eficacia de los procesos soportados por el sistema en cuestión.

1) 
Lic. Byron Alfredo Galindo Arauz
Auditor Gubernamental



1) 
Ing. Erickson Alexander Aqueche Padilla
Auditor Gubernamental



1) 
Lic. Angel Estuardo Sandoval Villatoro
Supervisor Gubernamental



Guatemala, Junio de 2019

REGISTRO NACIONAL DE LAS PERSONAS - RENAP
06 SEP 2019
SECRETARÍA GENERAL
OFICINAS CENTRALES RENAP
3do. piso, Av. 14-00

REGISTRO NACIONAL DE LAS PERSONAS - RENAP
SECRETARÍA GENERAL
06 SEP 2019
FRENTE: 14-00

