45

MARA CUARTA DE PRIMERA INSTANCIA DE LA CORTE DE CUENTAS DE LA REPUBLICA; San Salvador a las nueve horas con treinta y cinco minutos del siete de noviembre dos mil dieciséis.

El presente Juicio de Cuentas clasificado con el Número **JC-IV-56-2015** ha sido instruido en contra del señor **SERGIO MANOLO PADILLA FUNES,** Coordinador de Informática, con un salario mensual de *MIL CUATROCIENTOS CINCUENTA DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* $1,450.00; por su actuación según el **INFORME DE AUDITORÍA DE GESTIÓN A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN A LA PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS (PDDH), POR EL PERÍODO DEL UNO DE ENERO DOS MIL TRECE AL TREINTA Y UNO DE AGOSTO DE DOS MIL QUINCE;** conteniendo ocho Reparos con Responsabilidad Administrativa.

Ha intervenido en esta Instancia en representación del señor Fiscal General de la República la licenciada **MARIA DE LOS ANGELES LEMUS DE ALVARADO** en sustitución de la licenciada **ROXANA BEATRIZ SALGUERO RIVAS.**

LEIDOS LOS AUTOS;

Y, CONSIDERANDO:

I-) Por auto de **fs. 20** a **21** ambos vto., emitido a las diez horas y cinco minutos del día cuatro de enero de dos mil dieciséis; esta Cámara ordenó iniciar el Juicio de Cuentas en contra del servidor actuante antes expresado; el cual a fs. 22 fue notificado al señor Fiscal General de la República.

II-) A **fs. 23** la licenciada **ROXANA BEATRIZ SALGUERO RIVAS,** en su calidad de Agente Auxiliar del señor Fiscal General de la República, presentó

escrito mediante el cual se mostró parte, legitimando su personería con Credencial y Resolución que agregó a fs. 24 y 25; por lo que ésta Cámara mediante auto de fs. 25 vto., a 26 fte., emitido a las trece horas y cincuenta minutos del día diecinueve de enero de dos mil dieciséis, le tuvo por parte en el carácter en que compareció.

III-) Con base a lo establecido en los Artículos 66 y 67 de la Ley de esta Institución, esta Cámara elaboró el Pliego de Reparos, el cual corre agregado de **fs. 27 a fs. 34,** ambos **vto.**, emitido a las nueve horas del día dieciocho de marzo de dos mil dieciséis; ordenándose en el mismo emplazar a los servidores actuantes, para que acudieran a hacer uso de su Derecho de Defensa en el término establecido en el Artículo 68 de la Ley de la Corte de Cuentas de la República, y notificarle al señor Fiscal General de la República de la emisión del Pliego de Reparos, que esencialmente dice: **REPARO UNO. RESPONSABILIDAD ADMINISTRATIVA. PÉRDIDA DE INFORMACIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS.** Según el Informe de Auditoria, los Auditores comprobaron que en fecha dos de marzo de 2015, se originó una falla en el servidor de correos institucionales de la PDDH, ocasionando la suspensión del servicio y la pérdida total de información de aproximadamente 445 cuentas de usuarios de correo electrónico institucional de todas las dependencias de la entidad, no logrando efectuar la recuperación de la información institucional de los usuarios de sus cuentas de correo. **REPARO DOS. RESPONSABILIDAD ADMINISTRATIVA. SISTEMA INFORMÁTICO INTEGRADO DE GESTIÓN (SIIG) QUE APOYA A LOS PROCESOS SUSTANTIVOS DE LA PDDH ES INEFICIENTE E INEFECTIVO.** Según el Informe de Auditoria, los Auditores verificaron que el Sistema Informático Integrado de Gestión (SIIG) que apoya a los procesos sustantivos de la PDDH es inefectivo e ineficiente, debido a lo siguiente: a) El sistema SIIG no apoya a todos los procesos sustantivos que realiza la PDDH en función del proceso de la defensa para los derechos humanos, debido a que únicamente se registran las acciones de los procesos de toma de denuncia y orientación, dejando por fuera el registro de la asistencia y acompañamiento, monitoreo de privados de libertad, acciones de prevención para la defensa de los

46

derechos humanos, resoluciones efectuadas por los Delegados Locales y Departamentales, entre otros. b) El sistema SIIG no cubre las necesidades de información reales de la PDDH, debido a que las opciones de registro de los módulos para toma de denuncia y orientación no se apegan a la realidad de los procesos actuales. c) La información de los expedientes de tomas de denuncia y otras acciones no se almacenan de forma completa, efectuando la digitalizando de forma parcial, por lo que algunas diligencias o acciones evidenciadas en los expedientes físicos no se respaldan de forma digital. d) La operatividad del sistema SIIG en relación a los tiempos de respuesta es ineficiente debido a lentitud en el procesamiento y consulta, afectando la atención de los usuarios o víctimas de abuso de los derechos humanos que se acercan a la institución a solicitar ayuda. e) La seguridad de acceso al sistema por medio de la contraseña de acceso de ingreso (log in de usuario) y su contraseña no es confiable, ya que la entidad no cuenta con una política en la administración de cambio periódico de contraseñas para los usuarios del sistema, además las contraseñas utilizadas son las que inicialmente se asignaron a los usuarios desde la puesta en marcha del sistema en el año 2006. f) Adicional a las bandejas originales en el sistema SIIG para el alojamiento de los expedientes de los usuarios, se han creado bandejas denominadas "experimentales", en las cuales se están almacenando los expedientes del sistema y archivos digitalizados. Y g) Existe inconsistencia en la información de las resoluciones de denuncias que se registran en el sistema SIIG, debido a que únicamente se permite que las resoluciones sean las efectuadas por parte del Procurador General, aunque se ha autorizado a los Delegados regionales, Departamentales y Locales para poder emitir dichas resoluciones a nivel nacional, las cuales no se pueden registrar en el sistema, por lo que el sistema no dispone de información real y confiable para la toma de decisiones, que para el caso en particular, no reflejaría la cantidad de resoluciones que la PDDH ha efectuado sobre las denuncias a nivel nacional. **REPARO TRES. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONFIABILIDAD DE LAS BASES DE DATOS DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS PDDH.** Según el Informe de Auditoria los Auditores comprobaron que las bases de datos del Sistema Informático Integrado de Gestión (SIIG), Sistema de Información y Gestión de la Procuraduría (SIGEP) y Sistema de Información de Privados de Libertad, para el apoyo a los procesos sustantivos de la PDDH no son

confiables, debido a vulnerabilidades de seguridad física y lógica e integridad en la información de las bases, de acuerdo a los siguientes aspectos: a) La base de datos del Sistema Informático Integrado de Información (SIIG) de la PDDH no es confiable, debido entre otros aspectos a lo siguiente: i. La información contenida en los expedientes por denuncias u otras acciones relacionadas con la defensa de los derechos humanos no se almacenan completamente en la base de datos, cargando únicamente información parcial o mínima, para referencia de las diligencias o acciones contenida en los expedientes físicos. ii. Las resoluciones a denuncias efectuadas en el sistema por parte de los delegados departamentales o locales no se registran en el sistema como tal, por lo que en la base de datos no se refleja el dato exacto de las resoluciones efectuadas a nivel nacional, sino únicamente las efectuadas por el Procurador General. iii. La información del sistema SIGEP no fue migrada a la base de datos del SIIG, por lo tanto, la base de datos del mismo no cuenta con la información de 88,758 expedientes que incluye denuncias, orientaciones y gestiones de buenos oficios, recibidas y realizadas en cada delegación a nivel nacional, del período 1996 hasta el 2006. iv. El acceso y carga de la información de expedientes en la base de datos es lenta, sobrepasando los límites de tiempos razonables para el almacenamiento o búsqueda de los mismos. v. No se evidenció la existencia de un diccionario de datos para la base del SIIG. b) Verificaron que la base de datos del SIGEP no es confiable debido entre otros aspectos a lo siguiente: i. La base de datos del sistema SIGEP se encuentra almacenada en un equipo estacionario en la Unidad de Control de Procedimientos, el cual no cuenta con medidas de seguridad físicas ni lógicas para el resguardo de la información, que minimice el riesgo de hurto, daño o pérdida de información ejecutada por personal no autorizado, o desastres naturales. ii. No existen huellas de auditoría para el rastreo y registro de las actividades de los usuarios del sistema, sobre modificación, adición y eliminación de los registros de la base de datos del sistema SIGEP. c) comprobaron que el registro de las personas privadas de libertad del Departamento de Verificación Penitenciaria de la PDDH, no es confiable, debido entre otros aspectos a lo siguiente: i. El Departamento de Verificación Penitenciaria no cuenta con un sistema y base de datos para el registro centralizado de personas privadas de libertad y de centros autorizados de detención, que cuente con las medidas de seguridad que minimicen el riesgo de hurto, daño o pérdida de información ejecutada por personal no

autorizado o desastres naturales. II. Los datos con que cuenta la PDDH no garantizan que la información del registro de detenidos que a diario se ingresa, esté actualizada conforme a los datos o notificaciones que se remiten por escrito por las diferentes sedes policiales a nivel nacional, limitando la disponibilidad de información concerniente al tema de privados de libertad y poder dar expedita respuesta a las denuncias sobre personas desaparecidas o sobre la información actualizada de los detenidos en las bartolinas policiales a nivel nacional. **REPARO CUATRO. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONFIABILIDAD Y OBSOLESCENCIA DE LA PLATAFORMA TECNOLÓGICA DE LOS SERVIDORES CENTRALES QUE SOPORTAN LAS ACTIVIDADES DE PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN DE LOS SISTEMAS.** Según el Informe de Auditoria los Auditores comprobaron que existe obsolescencia en la plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de la información de los sistemas de apoyo a los procesos sustantivos y administrativos, así como los servicios informáticos, comunicaciones y seguridad de la red de la Procuraduría para la Defensa de los Derechos Humanos. **REPARO CINCO. RESPONSABILIDAD ADMINISTRATIVA. CARENCIA DE APROBACION DEL PLAN DE CONTINGENCIA POR LA MAXIMA AUTORIDAD.** Según el Informe de Auditoria los Auditores comprobaron que el Departamento de Informática de la PDDH no cuenta con un plan de contingencia aprobado por la Máxima Autoridad. **REPARO SEIS. RESPONSABILIDAD ADMINISTRATIVA. VULNERABILIDADES EN LA SEGURIDAD DE LA SALA DE RESGUARDO DE SERVIDORES CENTRALES INSTALADOS EN EL DEPARTAMENTO DE INFORMÁTICA.** Según el Informe de Auditoria los Auditores comprobaron, que existe vulnerabilidad en la seguridad física de la sala de resguardo de los servidores centrales institucionales instalados en el Departamento de Informática de la PDDH, los cuales proveen de los servicios informáticos (Sistemas administrativos y de apoyo a los procesos sustantivos, base de datos, página Web, correo electrónico institucional, sistemas de seguridad perimetral, entre otros) a los usuarios de la red tanto en la oficina central como en las delegaciones departamentales y locales. A continuación se detallan algunas de ellas, las cuales representan riesgos de acceso físico y desastres naturales: a) Vulnerabilidad en el acceso físico al Área de Servidores o el Data Center, ya que no cuenta con un área

específica para su alojamiento y resguardo, compartiendo actualmente el área utilizada por técnicos de informática. b) Las áreas de acceso no se encuentran restringidas, no poseen puertas con chapas electrónicas o biométricas para el control del ingreso del personal. c) No existen las medidas para el monitoreo de la seguridad (cámaras de video vigilancia, alarmas, detectores de humo, medidores de temperatura, medidores de humedad, entre otros). d) La infraestructura de servidores y rack de comunicaciones no se encuentran instalados sobre un piso falso o tarimas especiales que minimicen el riesgo de daños a los equipos en caso de terremotos, inundaciones o fugas de agua internamente, ya que se encuentran instalados en el mismo nivel del baño dentro de la Jefatura del Departamento de Informática. e) Cielos falsos sobre la ubicación de los gabinetes de servidores y rack de comunicaciones con señales de filtración de agua así como en el piso. f) En el área de servidores se encuentra resguardado equipo de cómputo inservible o por reparar, el cual puede servir de refugio y crianza de roedores u otro tipo de plagas, los cuales pueden dañar dichos servidores. g) Conexiones de cables eléctricos y cable estructurado (UTP) en desorden, exponiendo a los equipos a daños por alzas o bajas de la potencia eléctrica. **REPARO SIETE. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE SEGUIMIENTO A CONTRATACIÓN DE SERVICIOS DE INTERNET PARA GARANTIZAR LA EFICACIA DEL SERVICIO PRESTADO.** Según el Informe de Auditoria los Auditores comprobaron que durante el período comprendido del 1 de julio al 31 de diciembre de 2013, se contrató servicios de "Internet Dedicado" a través del Contrato No. 017/2013, de fecha 28 de junio de 2013 para los cuatro edificios de San Salvador, 13 delegaciones Departamentales y 4 delegaciones locales de la PDDH. Además, para el período del 1 de marzo de 2014 al 31 de diciembre de 2014, según Contrato No.019/2014 de fecha 28 de febrero de 2014, la contratación y la descripción del mismo servicio se mantuvo igual; sin embargo, al realizar visitas a las oficinas regionales de la PDDH en los municipios de Santa Tecla, Santa Ana, Ahuachapán, Cojutepeque, San Vicente, Zacatecoluca, Soyapango y Chalatenango, así como a diferentes Unidades Organizativas en oficina central, se verificó que dicho servicio contratado no satisfizo las necesidades de información de los usuarios debido, entre otros, a la limitantes en la carga y actualización de expedientes a las bases de datos del SIIG sobre denuncias, orientaciones y gestiones de buenos oficios recibidas y realizadas en

48

cada delegación departamental y local, así como en la operatividad del sistema que se conectan a los servidores a través de dichos enlaces, correo electrónico institucional y lentitud o indisponibilidad de navegación para la consulta de sitios web. Y **REPARO OCHO. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONTROL DE INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE.** Según el Informe de Auditoria, los Auditores comprobaron que el Departamento de Informática no tiene control sobre los procedimientos de instalación y desinstalación de software en los diferentes equipos informáticos de la PDDH, ya que no existe un detalle específico de los diferentes equipos estacionarios y portátiles (laptops) que detalle cuándo y a cuáles les fueron instalados los softwares que cuenten con sus respectivas licencias extendidas por el fabricante y compradas por la entidad para tal fin o con software libre.

IV-) A **fs. 35**, corre agregada la Esquela de Notificación efectuada al señor Fiscal General de la República; a **fs. 36**, corre agregado el Emplazamiento del funcionario actuante. La licenciada **MARIA DE LOS ANGELES LEMUS DE ALVARADO,** en su calidad de Agente Auxiliar del señor Fiscal General de la República a fs. 39, presentó escrito mediante el cual se mostró parte, legitimando su personería con Credencial y Resolución que agregó a fs. 40 y 41; por lo que ésta Cámara mediante auto de fs. 42 vto., a 43 fte., emitido a las ocho horas y treinta minutos del día ocho de junio de dos mil dieciséis, se le tuvo por parte en el carácter en que compareció en sustitución de la licenciada **ROXANA BEATRIZ SALGUERO RIVAS.**

V-) Por auto emitido a las nueve horas y treinta minutos del día veintisiete de abril de dos mil dieciséis de **fs. 36 vto., a fs. 37 fte,** se declaró Rebelde al señor **SERGIO MANOLO PADILLA FUNES,** y se concedió Audiencia a la Fiscalía General de la Republica.

CORTE DE CUENTAS DE LA REPÚBLICA · CAMARA DE PRIMERA INSTANCIA · EL SALVADOR, C.A.

VI-) A **fs. 39**, fue evacuada la opinión solicitada a la Fiscalía General de la República, por la licenciada **MARIA DE LOS ANGELES LEMUS DE ALVARADO,** en la cual expreso: *"REPARO UNO. PERDIDA DE INFORMACION DE LAS CUENTAS DE CORREO ELECTRONICO DE LA PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS. REPARO DOS. SISTEMA INFORMATICO INTEGRADO DE GESTION (SIIG) QUE APOYA A LOS PROCESOS SUSTANTIVOS DE LA PDDH ES INEFICIENTE E INEFECTIVO. REPARO TRES. FALTA DE CONFIABILIDAD DE LAS BASES DE DATOS DE LA PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS. REPARO CUATRO. FALTA DE CONFIABILIDAD Y OBSOLESCENCIA DE LA PLATAFORMA TECNOLOGICA DE LOS SERVIDORES CENTRALES QUE SOPORTAN LAS ACTIVIDADES DE PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACION DE LOS SISTEMAS. REPARO CINCO. CARENCIA DE APROBACION DEL PLAN DE CONTINGENCIA POR LA MAXIMA AUTORIDAD. REPARO SEIS. VULNERABILIDADES EN LA SEGURIDAD DE LA SALA DE RESGUARDO DE SERVIDORES CENTRALES INSTALADOS EN EL DEPARTAMENTO DE INFORMATICA. REPARO SIETE. FALTA DE SEGUIMIENTO A CONTRATACION DE SERVICIOS DE INTERNET PARA GARANTIZAR LA EFICACIA DEL SERVICIO PRESTADO. REPARO OCHO. FALTA DE CONTROL DE INSTALACION Y DESINSTALACION DE SOFTWARE. En el presente juicio, el servidor no ha contestado el pliego correspondiente ni ha presentado documentación probatoria tendiente a desvirtuar los hallazgos; siendo este el momento procesal oportuno para hacer uso de las garantías constitucionales que se le otorgan a efecto de demostrar la transparencia de su gestión en la PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS (PDDH), por el periodo comprendido del uno de enero de dos mil trece al treinta y uno de agosto de dos mil quince; por tanto, la Representación Fiscal es de la opinión que ante la falta de prueba a valorar los reparos se mantienen, y se solicita que en sentencia el señor SERGIO MANOLO PADILLA FUNES sea condenado al pago de la Responsabilidad Administrativa a favor del Estado de El Salvador, de conformidad a lo establecido en los artículos 54 y 69 de la Ley de la Corte de Cuentas de la República"""".* Por Auto emitido a las ocho horas y treinta minutos del día ocho de junio de dos mil dieciséis de **fs. 42 vto., a fs. 43 fte,** se tuvo por parte a la licenciada **Lemus de Alvarado,** en sustitución de la licenciada **Roxana Beatriz Salguero Rivas**, y se dio por evacuada la opinión de la Fiscalía General de la Republica, ordenándose emitir la respectiva sentencia.

49

VII-) Luego de analizado el informe de auditoría, Papeles de Trabajo y Opinión Fiscal; es fundamental hacerle saber a las partes procesales la importancia de la presente sentencia, en el sentido que esta Cámara garante de los derechos que les ampara a los servidores actuantes, así como también de Principios y Garantías constitucionales, se permite señalar que en la presente motivación toma en cuenta todos y cada uno de los elementos fácticos y jurídicos del proceso, considerados individual y conjuntamente, con apego a las reglas de la sana crítica, según lo prescribe el **Artículo 216** del Código Procesal Civil y Mercantil, en ese sentido, supone la obligación de todo Tribunal de Justicia, de exponer las razones y argumentos que conducen al fallo, sobre los antecedentes de hecho y los fundamentos de derecho que lo sustentan, tal y como lo prescribe el **Artículo 69** de la Ley de la Corte de Cuentas de la República con relación al **Artículo 217** del Código Procesal Civil y Mercantil, con ello se fundamenta la convicción respecto a los medios probatorios que desfilaron durante el juicio, y que en atención judicial se hace posible el contacto directo con ellos y su valoración, por tanto, esta Cámara basada en los criterios antes expuestos emite las siguientes consideraciones: **REPARO UNO. RESPONSABILIDAD ADMINISTRATIVA. PÉRDIDA DE INFORMACIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS.** Según el Informe de Auditoria en fecha dos de marzo de 2015 se originó una falla en el servidor de correos institucionales de la PDDH, ocasionando la suspensión del servicio y la pérdida total de información de aproximadamente 445 cuentas de usuarios de correo electrónico institucional de todas las dependencias de la entidad, no logrando efectuar la recuperación de la información institucional de los usuarios de sus cuentas de correo. El señor **SERGIO MANOLO PADILLA FUNES,** según consta a fs. 36 fue emplazado, no obstante no ejerció su derecho de defensa en el término de ley, por lo cual fue declarado rebelde según auto de fs. 37 fte, estado que no interrumpió en el presente proceso, no teniendo así explicaciones o comentarios en los reparos atribuidos a su persona. Siendo estos los reparos uno, dos, tres, cuatro, cinco, seis, siete y ocho. Por su parte la **Representación Fiscal**, en su opinión de mérito lo hizo de manera general para todos los reparos atribuidos, considerando que el servidor no contesto el pliego correspondiente ni presento documentación probatoria tendiente a desvirtuar los hallazgos, siendo este el momento procesal

oportuno para hacer uso de las garantías constitucionales que se le otorgan a efecto de demostrar la transparencia de su gestión, por lo que ante la falta de prueba que valorar, los reparos deben mantenerse. Sobre lo antes expuesto **los suscritos Jueces** consideramos que respecto a la condición señalada, al revisar los papeles de trabajo bajo referencia ACR10 constatamos que se encuentran los memorándum y notas dirigidas al encargado del Departamento de Informática, en las cuales se le solicitó el informe sobre la situación real de la falta de acceso al correo institucional, no así los documentos que demostraren las gestiones realizadas para solucionar tales fallas, pues se señaló que esta se debió a que el Coordinador del Departamento de Informática no efectuó pruebas de la configuración para la contingencia basada en un arreglo de discos RAID, para garantizar que toda la información se encontrara respaldada en las dos unidades de disco del servidor de correo electrónico, incumpliéndose el Art. 40 del Reglamento para el Uso y Control de Tecnologías de Información y Comunicación en las Entidades del Sector Publico emitido por la Corte de Cuentas de la Republica, el cual establece: *"El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, perdida de información u otras situaciones similares",* asimismo se incumplió el Art. 35 del Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos; en razón de lo anterior y al no existir alegatos o explicaciones sobre lo atribuido por parte del servidor actuante y documentación que desvirtúe lo señalado, de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República el **reparo se confirma** y procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas de la República, con el diez por ciento **10%** del salario mensual devengado en el periodo auditado. **REPARO DOS. RESPONSABILIDAD ADMINISTRATIVA. SISTEMA INFORMÁTICO INTEGRADO DE GESTIÓN (SIIG) QUE APOYA A LOS PROCESOS SUSTANTIVOS DE LA PDDH ES INEFICIENTE E INEFECTIVO.** Según el Informe de Auditoria los Auditores verificaron que el Sistema Informático Integrado de Gestión (SIIG) que apoya a los procesos sustantivos de la PDDH es inefectivo e ineficiente, debido a lo siguiente: **a)** El sistema SIIG no apoya a todos los procesos sustantivos que realiza la PDDH en

función del proceso de la defensa para los derechos humanos, debido a que únicamente se registran las acciones de los procesos de toma de denuncia y orientación, dejando por fuera el registro de la asistencia y acompañamiento, monitoreo de privados de libertad, acciones de prevención para la defensa de los derechos humanos, resoluciones efectuadas por los Delegados Locales y Departamentales, entre otros. **b)** El sistema SIIG no cubre las necesidades de información reales de la PDDH, debido a que las opciones de registro de los módulos para toma de denuncia y orientación no se apegan a la realidad de los procesos actuales. **c)** La información de los expedientes de tomas de denuncia y otras acciones no se almacenan de forma completa, efectuando la digitalizando de forma parcial, por lo que algunas diligencias o acciones evidenciadas en los expedientes físicos no se respaldan de forma digital. **d)** La operatividad del sistema SIIG en relación a los tiempos de respuesta es ineficiente debido a lentitud en el procesamiento y consulta, afectando la atención de los usuarios o víctimas de abuso de los derechos humanos que se acercan a la institución a solicitar ayuda. **e)** La seguridad de acceso al sistema por medio de la contraseña de acceso de ingreso (log in de usuario) y su contraseña no es confiable, ya que la entidad no cuenta con una política en la administración de cambio periódico de contraseñas para los usuarios del sistema, además las contraseñas utilizadas son las que inicialmente se asignaron a los usuarios desde la puesta en marcha del sistema en el año 2006. **f)** Adicional a las bandejas originales en el sistema SIIG para el alojamiento de los expedientes de los usuarios, se han creado bandejas denominadas "experimentales", en las cuales se están almacenando los expedientes del sistema y archivos digitalizados, y **g)** Existe inconsistencia en la información de las resoluciones de denuncias que se registran en el sistema SIIG, debido a que únicamente se permite que las resoluciones sean las efectuadas por parte del Procurador General, aunque se ha autorizado a los Delegados regionales, Departamentales y Locales para poder emitir dichas resoluciones a nivel nacional, las cuales no se pueden registrar en el sistema, por lo que el sistema no dispone de información real y confiable para la toma de decisiones, que para el caso en particular, no reflejaría la cantidad de resoluciones que la PDDH ha efectuado sobre las denuncias a nivel nacional. Los **suscritos Jueces** en relación a lo señalado por el auditor, estimamos que la condición de mérito deviene de la ineficiencia e inefectividad del sistema informático integrado de gestión que apoya

a los procesos sustantivos de la Procuraduría para la Defensa de los Derechos Humanos; el Art. 15 del Reglamento para el Uso y Control de Tecnologías de Información y Comunicación en las Entidades del Sector Publico, emitido por la Corte de Cuentas de la Republica, dice: *"la Unidad de TIC implementará la metodología para el ciclo de vida del desarrollo de sistemas, asegurando que los sistemas de información sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada";* en ese sentido tal disposición claramente establece que dicho sistema debe ser eficaz y eficiente; según comentarios del servidor en la etapa de auditoria y que constan en el Informe de Auditoria, expreso que había planificado un cronograma de actividades a fin de superar las deficiencias importantes y de impacto, y para ello se planeó formar un equipo de desarrollo de Sistemas con estudiantes de Horas sociales para sustentar estas gestiones; en ese sentido es importante mencionar que el Art. 314 ordinal 1° del Código Procesal Civil y Mercantil establece: *"no requieren ser probados: los hechos admitidos o estipulados por las partes"*, de acuerdo a lo anterior es claro que dicho servidor al momento de la Auditoria admitió expresamente la deficiencia señalada por lo que es conforme a derecho a concluir que el **reparo se confirma** de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República y procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas de la República, con el diez por ciento **10%** del salario mensual devengado en el periodo auditado. **REPARO TRES. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONFIABILIDAD DE LAS BASES DE DATOS DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS PDDH.** Según el Informe de Auditoria los Auditores comprobaron que las bases de datos del Sistema Informático Integrado de Gestión (SIIG), Sistema de Información y Gestión de la Procuraduría (SIGEP) y Sistema de Información de Privados de Libertad, para el apoyo a los procesos sustantivos de la PDDH no son confiables, debido a vulnerabilidades de seguridad física y lógica e integridad en la información de las bases, de acuerdo a los siguientes aspectos: **a)** La base de datos del Sistema Informático Integrado de Información (SIIG) de la PDDH no son confiables, debido entre otros aspectos a lo siguiente: **i.** La información contenida en los expedientes por denuncias u otras acciones relacionadas con la defensa de los derechos humanos no se almacenan completamente en la base de datos, cargando únicamente información parcial o

mínima, para referencia de las diligencias o acciones contenida en los expedientes físicos. **ii.** Las resoluciones a denuncias efectuadas en el sistema por parte de los delegados departamentales o locales no se registran en el sistema como tal, por lo que en la base de datos no se refleja el dato exacto de las resoluciones efectuadas a nivel nacional, sino únicamente las efectuadas por el Procurador General. **iii.** La información del sistema SIGEP no fue migrada a la base de datos del SIIG, por lo tanto, la base de datos del mismo no cuenta con la información de 88,758 expedientes que incluye denuncias, orientaciones y gestiones de buenos oficios, recibidas y realizadas en cada delegación a nivel nacional, del período 1996 hasta el 2006. **iv.** El acceso y carga de la información de expedientes en la base de datos es lenta, sobrepasando los límites de tiempos razonables para el almacenamiento o búsqueda de los mismos. **v.** No se evidenció la existencia de un diccionario de datos para la base del SIIG. **b)** Verificaron que la base de datos del SIGEP no es confiable debido entre otros aspectos a lo siguiente: **i.** La base de datos del sistema SIGEP se encuentra almacenada en un equipo estacionario en la Unidad de Control de Procedimientos, el cual no cuenta con medidas de seguridad físicas ni lógicas para el resguardo de la información, que minimice el riesgo de hurto, daño o pérdida de información ejecutada por personal no autorizado, o desastres naturales. **ii.** No existen huellas de auditoría para el rastreo y registro de las actividades de los usuarios del sistema, sobre modificación, adición y eliminación de los registros de la base de datos del sistema SIGEP. **c)** comprobaron que el registro de las personas privadas de libertad del Departamento de Verificación Penitenciaria de la PDDH, no es confiable, debido entre otros aspectos a lo siguiente: **i.** El Departamento de Verificación Penitenciaria no cuenta con un sistema y base de datos para el registro centralizado de personas privadas de libertad y de centros autorizados de detención, que cuente con las medidas de seguridad que minimicen el riesgo de hurto, daño o pérdida de información ejecutada por personal no autorizado o desastres naturales. **II.** Los datos con que cuenta la PDDH no garantizan que la información del registro de detenidos que a diario se ingresa, esté actualizada conforme a los datos o notificaciones que se remiten por escrito por las diferentes sedes policiales a nivel nacional, limitando la disponibilidad de información concerniente al tema de privados de libertad y poder dar expedita respuesta a las denuncias sobre personas desaparecidas o sobre la información actualizada de los detenidos en las bartolinas policiales a nivel

nacional. Sobre lo antes expuesto **los suscritos Jueces** al revisar los papeles de trabajo bajo referencia ACR10 verificamos la nota enviada por el encargado del Departamento de Informática, en la cual hace ver que al momento de la Auditoria estaban conscientes de la falta de confiabilidad del sistema, sosteniendo que se realizaron algunas gestiones para subsanar dicha deficiencia; sin embrago afirma de igual manera que no se contaba todavía con ciertos elementos para optimizar su mejor funcionabilidad en los procesos sustantivos llevados por la Institución; el Art. 35 del Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el Diario Oficial no. 85, Tomo 399, de fecha 13 de mayo de 2013, establece lo siguiente: Sección Cuarta. Del Departamento de Informática. *"Son funciones de este Departamento, las siguientes: 1. Proponer al Procurador o Procuradora los sistemas de información electrónica de la Institución, a efecto de satisfacer las necesidades de procesamiento de información y datos, así como su distribución y control. 2. Realizar las copias de respaldo necesarias de los sistemas de almacenamiento de información electrónica de la Procuraduría. 8. Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional...";* disposiciones legales incumplidas por el servidor, en razón de lo anterior y al no existir documentación que compruebe las gestiones realizadas por el servidor, que garanticen la confiabilidad de la información, es procedente **confirmar el reparo** de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República y procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas de la República, con el diez por ciento **10%** del salario mensual devengado en el periodo auditado. **REPARO CUATRO. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONFIABILIDAD Y OBSOLESCENCIA DE LA PLATAFORMA TECNOLÓGICA DE LOS SERVIDORES CENTRALES QUE SOPORTAN LAS ACTIVIDADES DE PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN DE LOS SISTEMAS.** Según el Informe de Auditoria, existe obsolescencia en la plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de la información de los sistemas de apoyo a los procesos sustantivos y administrativos, así como los servicios informáticos, comunicaciones y seguridad de la red de la Procuraduría para la Defensa de los

52

Derechos Humanos. En el caso que nos ocupa, los **suscritos Jueces** consideramos pertinente aclarar que la observación señalada en el caso de mérito se refiere a la obsolescencia en la plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de la información de los sistemas de apoyo a los procesos sustantivos y administrativos; al revisar los papales de trabajo bajo referencia ACR10 constan notas enviadas por el coordinador de informática, informando sobre fallas de la plataforma tecnológica de los servidores centrales de la institución, asimismo consta la solicitud de compra por parte del Departamento de Informática de dos servidores con ciertas características específicas para un mejor funcionamiento, con dicha acción los suscritos estimamos que el servidor ha cumplido con lo establecido en Art. 13 del Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República, establece lo siguiente: *"La Unidad de TIC, efectuará diagnóstico de las necesidades y requerimientos tecnológicos de las dependencias de la Entidad y deberá proyectar las mejoras de las tecnologías de información y comunicaciones, considerando los costos de transición, viabilidad, capacidad técnica, instalaciones, riesgos tecnológicos, vida útil y tasas de crecimiento de la infraestructura tecnológica",* siendo importante dejar establecido que el auditor no determino de forma precisa cuales equipos estaban obsoletos, lo cual es importante para los suscritos, ya que desconocemos a que equipos se refiere en la condición, razón por la cual se concluye que **reparo se desvanece** de conformidad al Art. 69 Inc. 1 de la Ley de la Corte de Cuentas de la República. **REPARO CINCO. RESPONSABILIDAD ADMINISTRATIVA. CARENCIA DE APROBACION DEL PLAN DE CONTINGENCIA POR LA MAXIMA AUTORIDAD.** Según el Informe de Auditoria, el Departamento de Informática de la PDDH no cuenta con un plan de contingencia aprobado por la Máxima Autoridad. Sobre lo antes señalado los **suscritos Jueces,** al revisar los papeles de trabajo bajo referencia ACR10, constatamos el plan anual remitido por el coordinador de informática, que se encontraba en revisión previa a su aprobación; el Art. 39 del Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República, dice *"La Unidad de TIC, **deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad**, este plan*

debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la Entidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año. Deberá ser comunicado a los niveles pertinentes"; con fundamento en lo anterior, concluimos que la norma es clara en establecer que será la Máxima Autoridad de la Institución la encargada de autorizar el Plan de Contingencia, por lo que no corresponde al Coordinador de Informática dicha autorización; constatándose en papeles de trabajo que si se contaba con el Plan señalado por el Auditor en la condición de mérito, por lo que es conforme **desvanecer el reparo** de conformidad al Art. 69 Inc. 1 de la Ley de la Corte de Cuentas de la República. **REPARO SEIS. RESPONSABILIDAD ADMINISTRATIVA. VULNERABILIDADES EN LA SEGURIDAD DE LA SALA DE RESGUARDO DE SERVIDORES CENTRALES INSTALADOS EN EL DEPARTAMENTO DE INFORMÁTICA.** Según el Informe de Auditoria los Auditores comprobaron, que existe vulnerabilidad en la seguridad física de la sala de resguardo de los servidores centrales institucionales instalados en el Departamento de Informática de la PDDH, los cuales proveen de los servicios informáticos (Sistemas administrativos y de apoyo a los procesos sustantivos, base de datos, página Web, correo electrónico institucional, sistemas de seguridad perimetral, entre otros) a los usuarios de la red tanto en la oficina central como en las delegaciones departamentales y locales. A continuación se detallan algunas de ellas, las cuales representan riesgos de acceso físico y desastres naturales**: a)** Vulnerabilidad en el acceso físico al Área de Servidores o el Data Center, ya que no cuenta con un área específica para su alojamiento y resguardo, compartiendo actualmente el área utilizada por técnicos de informática. **b)** Las áreas de acceso no se encuentran restringidas, no poseen puertas con chapas electrónicas o biométricas para el control del ingreso del personal. **c)** No existen las medidas para el monitoreo de la seguridad (cámaras de video vigilancia, alarmas, detectores de humo, medidores de temperatura, medidores de humedad, entre otros). **d)** La infraestructura de servidores y rack de comunicaciones no se encuentran instalados sobre un piso falso o tarimas especiales que minimicen el riesgo de daños a los equipos en caso

de terremotos, inundaciones o fugas de agua internamente, ya que se encuentran instalados en el mismo nivel del baño dentro de la Jefatura del Departamento de Informática. **e)** Cielos falsos sobre la ubicación de los gabinetes de servidores y rack de comunicaciones con señales de filtración de agua así como en el piso. **f)** En el área de servidores se encuentra resguardado equipo de cómputo inservible o por reparar, el cual puede servir de refugio y crianza de roedores u otro tipo de plagas, los cuales pueden dañar dichos servidores. **g)** Conexiones de cables eléctricos y cable estructurado (UTP) en desorden, exponiendo a los equipos a daños por alzas o bajas de la potencia eléctrica. Los **suscritos Jueces,** al examinar los comentarios del Auditor, según nota de respuesta de fecha nueve de diciembre de dos mil quince suscrita por el coordinador de informática, en la cual admite las deficiencias señaladas por el Auditor, incumpliendo el Art. 27 del Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República, que dice: *"La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, Switch y otros dispositivos"";* en esta instancia el servidor no ejerció su derecho de defensa, quien no presento documentación y explicaciones sobre lo atribuido, por lo que es conforme a derecho concluir que **reparo se confirma** de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República y Art. 314 numeral 1° del Código Procesal Civil y Mercantil, procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas de la República, con el diez por ciento **10%** del salario mensual devengado en el periodo auditado. **REPARO SIETE. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE SEGUIMIENTO A CONTRATACIÓN DE SERVICIOS DE INTERNET PARA GARANTIZAR LA EFICACIA DEL SERVICIO PRESTADO.** Según el Informe de Auditoria, durante el período comprendido del 1 de julio al 31 de diciembre de 2013, se contrató servicios de ´Internet Dedicado´ a través del Contrato No. 017/2013, de fecha 28 de junio de 2013 para los cuatro edificios de San Salvador, 13 delegaciones Departamentales y 4 delegaciones locales de la

PDDH. Además, para el período del 1 de marzo de 2014 al 31 de diciembre de 2014, según Contrato No.019/2014 de fecha 28 de febrero de 2014, la contratación y la descripción del mismo servicio se mantuvo igual; sin embargo, al realizar visitas a las oficinas regionales de la PDDH en los municipios de Santa Tecla, Santa Ana, Ahuachapán, Cojutepeque, San Vicente, Zacatecoluca, Soyapango y Chalatenango, así como a diferentes Unidades Organizativas en oficina central, se verificó que dicho servicio contratado no satisfizo las necesidades de información de los usuarios debido, entre otros, a la limitantes en la carga y actualización de expedientes a las bases de datos del SIIG sobre denuncias, orientaciones y gestiones de buenos oficios recibidas y realizadas en cada delegación departamental y local, así como en la operatividad del sistema que se conectan a los servidores a través de dichos enlaces, correo electrónico institucional y lentitud o indisponibilidad de navegación para la consulta de sitios web. Sobre lo antes señalado como se ha expresado en los reparos precedentes, el servidor fue legalmente emplazado en el presente Juicio, no obstante no ejerció su derecho de defensa y fue declarado rebelde, estado que no interrumpió en el transcurso del proceso; el Art. 27 del Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República, dice: *"La Unidad de TIC deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica";* es decir debe emitir ***"mecanismos que controlen, verifiquen e identifiquen que el servicio o producto contratado sea el requerido y necesario para cubrir las necesidades solicitadas"***. Los suscritos al verificar los papeles de trabajo constatamos que no existe ningún procedimiento de control, y en esta instancia tampoco se anexo prueba que controvierta lo reportado por el auditor, por lo que se concluye que el **reparo se confirma** de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República y procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas de la República con el diez por ciento **10%** del salario mensual devengado en el periodo auditado. Y **REPARO OCHO. RESPONSABILIDAD ADMINISTRATIVA. FALTA DE CONTROL DE INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE.** Según el

Informe de Auditoria, los Auditores comprobaron que el Departamento de Informática no tiene control sobre los procedimientos de instalación y desinstalación de software en los diferentes equipos informáticos de la PDDH, ya que no existe un detalle específico de los diferentes equipos estacionarios y portátiles (laptops) que detalle cuándo y a cuáles les fueron instalados los softwares que cuenten con sus respectivas licencias extendidas por el fabricante y compradas por la entidad para tal fin o con software libre. El servidor relacionado como se ha mencionado, fue legalmente emplazado en el presente Juicio, no obstante no ejerció su derecho de defensa y fue declarado rebelde, estado que no interrumpió en el transcurso del proceso; sin embargo durante la fase de auditoria comentó que el Departamento de Informática había planificado superar las observaciones con la solicitud de servicio que se establece en los TDR del proceso de Libre Gestión No. 341/2015 referente al *"Suministro de equipo Informático (Equipos de protección perimetral, servidores y Access point) y licencias de software antivirus",* en el cual se solicita la configuración y ejecución del servicio del Directorio Activo para los equipos servidores, lo que técnicamente permitiría poder administrar los servicios, recursos, usuarios, etc. que formen parte del nuevo dominio a configurar; sin embargo no consta ningún documento que dé cumplimiento a lo que exige el Art. 45 y 47 del Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República, en ese sentido se incumplió lo establecido en el Art. 45 que dice: *"Todo el software instalado en la entidad, deberá estar amparado con la respectiva licencia extendida por el fabricante, otorgado a la entidad el derecho de instalación y uso de los mismos, de conformidad a lo establecido por la ley",* y el Art. 47 que establece: *"La Unidad de TIC es la responsable de la instalación de software libre, debiendo justificar los usuarios las necesidades de su uso",* entendiéndose que dicha unidad debía tener un control sobre los mismo, para lo cual debía implementar procedimientos de control, siendo este aquellos ***"mecanismos que sirven para controlar, verificar e identificar que el servicio o producto contratado sea el requerido y necesario para cubrir las necesidades solicitadas"***. En razón de ello se concluye que el **reparo se confirma** de conformidad al Art. 69 Inc. 2 de la Ley de la Corte de Cuentas de la República y procede la aplicación de multa de acuerdo a los criterios contenidos en el Art. 107 de la Ley de la Corte de Cuentas

de la República con el diez por ciento **10%** del salario mensual devengado en el periodo auditado.

POR TANTO: De acuerdo a los Considerandos anteriores y de conformidad con los artículos 195 No. 3 de la Constitución de la República, 3, 15, 16, 54, 55, 69, 107 y 115 de la Ley de la Corte de Cuentas de la República, 215, 216, 217 y 218 del Código Procesal Civil y Mercantil y demás disposiciones citadas en el reparo, a nombre de la República de El Salvador, esta Cámara Falla: **I-)** Declarase **Responsabilidad Administrativa,** por el **REPARO UNO** titulado ***"PÉRDIDA DE INFORMACIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **II-)** Declarase **Responsabilidad Administrativa,** por el **REPARO DOS** titulado ***"SISTEMA INFORMÁTICO INTEGRADO DE GESTIÓN (SIIG) QUE APOYA A LOS PROCESOS SUSTANTIVOS DE LA PDDH ES INEFICIENTE E INEFECTIVO",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **III-)** Declarase **Responsabilidad Administrativa,** por el **REPARO TRES** titulado ***"FALTA DE CONFIABILIDAD DE LAS BASES DE DATOS DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS PDDH",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **IV-)** Declarase Desvanecida la **Responsabilidad Administrativa,** por el **REPARO CUATRO** titulado ***"FALTA DE CONFIABILIDAD Y OBSOLESCENCIA DE LA PLATAFORMA TECNOLÓGICA DE LOS SERVIDORES CENTRALES QUE SOPORTAN LAS ACTIVIDADES DE***

55

PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN DE LOS SISTEMAS", absuélvase del pago de multa al señor **SERGIO MANOLO PADILLA FUNES. V-)** Declarase Desvanecida la **Responsabilidad Administrativa,** por el **REPARO CINCO** titulado ***"CARENCIA DE APROBACION DEL PLAN DE CONTINGENCIA POR LA MAXIMA AUTORIDAD", absuélvase*** del pago de multa al señor **SERGIO MANOLO PADILLA FUNES. VI-)** Declarase **Responsabilidad Administrativa,** por el **REPARO SEIS** titulado ***"VULNERABILIDADES EN LA SEGURIDAD DE LA SALA DE RESGUARDO DE SERVIDORES CENTRALES INSTALADOS EN EL DEPARTAMENTO DE INFORMÁTICA",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **VII-)** Declarase **Responsabilidad Administrativa,** por el **REPARO SIETE** titulado ***"FALTA DE SEGUIMIENTO A CONTRATACIÓN DE SERVICIOS DE INTERNET PARA GARANTIZAR LA EFICACIA DEL SERVICIO PRESTADO",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **VIII-)** Declarase **Responsabilidad Administrativa,** por el **REPARO OCHO** titulado ***"FALTA DE CONTROL DE INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE",*** en consecuencia ***condenase*** a pagar en concepto de Multa por la Infracción cometida al señor **SERGIO MANOLO PADILLA FUNES,** la cantidad de *CIENTO CUARENTA Y CINCO DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$145.00**, cantidad equivalente al 10 % del salario mensual devengado en el período auditado. **IX-)** Haciendo un total de **Responsabilidad Administrativa** la cantidad de *OCHOCIENTOS SETENTA DOLARES DE LOS ESTADOS UNIDOS DE AMERICA* **$870.00. X)** Dejase **PENDIENTE** de aprobación de la gestión al señor **SERGIO MANOLO PADILLA FUNES** por su actuación como Coordinador de Informática en el **INFORME DE AUDITORÍA DE GESTIÓN A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN A LA PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS**

(PDDH), POR EL PERÍODO DEL UNO DE ENERO DE DOS MIL TRECE AL TREINTA Y UNO DE AGOSTO DE DOS MIL QUINCE.

NOTIFIQUESE.

Ante mí,

Secretaria de Actuaciones.

JC-IV-56-2015
HAC
REF. FISCAL: 20-DE-UJC-12-2016
Licda. Roxana Beatriz Salguero Rivas

MARA CUARTA DE PRIMERA INSTANCIA DE LA CORTE DE CUENTAS DE LA REPUBLICA: San Salvador, a las nueve horas y veinte minutos del día cuatro de enero de dos mil diecisiete.

Transcurrido el termino establecido de conformidad con el Art. 70 de la Ley de la Corte de Cuentas de la República, sin que se haya interpuesto Recurso alguno sobre la Sentencia Definitiva pronunciada por esta Cámara a las nueve horas con treinta y cinco minutos del día siete de noviembre de dos mil dieciséis, agregada de folios 44 a folios 55 ambos vuelto del presente Juicio, declárese ejecutoriada dicha sentencia y líbrese la ejecutoria correspondiente.

NOTIFIQUESE.

CORTE DE CUENTAS DE LA REPÚBLICA - CÁMARA CUARTA DE PRIMERA INSTANCIA - EL SALVADOR, C.A.

Ante Mí,

Secretario de Actuaciones.

JC-IV-56-2015
HAC
REF. FISCAL: 20-DE-UJC-12-2016
Licda. Roxana Beatriz Salguero Rivas

CORTE DE CUENTAS DE LA REPÚBLICA

DIRECCION DE AUDITORÍA SIETE

INFORME DE AUDITORÍA DE GESTIÓN A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN A LA PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS (PDDH), POR EL PERÍODO DEL 1 DE ENERO 2013 AL 31 DE AGOSTO 2015

SAN SALVADOR, 21 DE DICIEMBRE DE 2015

INDICE

CORTE DE CUENTAS DE LA REPÚBLICA

1. RESUMEN EJECUTIVO

Señor
Procurador para la Defensa de los Derechos Humanos
Presente.

Hemos realizado Auditoría de Gestión a las Tecnologías de Información y Comunicación a la Procuraduría para la Defensa de los Derechos Humanos (PDDH), por el período del 1 de enero de 2013 al 31 de agosto 2015 y como resultado identificamos y hemos incorporado en el Informe de Auditoría, ocho hallazgos de auditoría cuyos títulos son los siguientes:

Área 1. Sistemas Informáticos de Apoyo a los Procesos Sustantivos de la PDDH

1) Pérdida de Información de las cuentas de Correo Electrónico de la Procuraduría para la Defensa de los Derechos Humanos.
2) Sistema informático integrado de gestión (SIIG) que apoya a los procesos sustantivos de la PDDH es ineficiente e inefectivo.
3) Falta de confiabilidad de las bases de datos de la Procuraduría para la Defensa de los Derechos Humanos.

Área 2. Infraestructura de Servidores y Seguridad de Plataforma

1. Falta de confiabilidad y obsolescencia de la plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de información de los sistemas.
2. Carencia de aprobación del plan de contingencia por la máxima autoridad.
3. Vulnerabilidades en la seguridad de la sala de resguardo de servidores centrales instalados en el Departamento de Informática.

Área 3. Planificación y Organización de las TIC´S

1) Falta de Seguimiento a Contratación de servicios de Internet para garantizar la eficacia del servicio prestado.
2) Falta de control de instalación y desinstalación de software.

Este informe contiene además, tres recomendaciones que deben ser cumplidas por la PDDH, tal como lo regula el Artículo 48 de la Ley de la Corte de Cuentas de la República.

San Salvador, 21 de diciembre de 2015.

DIOS UNIÓN LIBERTAD

Dirección de Auditoría Siete

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

2. PÁRRAFO INTRODUCTORIO

Señor
Procurador para la Defensa de los Derechos Humanos
Presente.

Con base al Art. 5 numeral 4, Art. 30 numerales 4, 5 y 6 y Art. 31 de la Ley de la Corte de Cuentas de la República, así como al Plan Anual de Trabajo de la Dirección de Auditoría Siete, mediante la Orden de Trabajo No. 33/2015, de fecha 27 de julio de 2015, efectuamos Auditoría de Gestión a las Tecnologías de Información y Comunicación a la Procuraduría para la Defensa de los Derechos Humanos (PDDH), por el período del 1 de enero de 2013 al 31 de agosto 2015.

3. OBJETIVOS Y ALCANCE DE LA AUDITORÍA

3.1 Objetivo General

Emitir un informe que contenga los resultados obtenidos de la evaluación constructiva y objetiva a la gestión de las Tecnologías de Información y Comunicación (TIC) de la Procuraduría para la Defensa de los Derechos Humanos, con el fin de determinar el grado de economía, eficiencia, eficacia y efectividad en el manejo de los recursos de tecnología de información y comunicación, la confiabilidad de los sistemas de información y el grado de apoyo a los procesos operativos y administrativos institucionales, por el período del 1 de enero de 2013 al 31 de agosto 2015.

3.2 Objetivos Específicos

a) Verificar que la infraestructura tecnológica de la PDDH esté capacitada para sostener los servicios a los usuarios.
b) Verificar el cumplimiento de objetivos y metas de los planes operativos y estratégicos institucionales relacionados con las TIC.
c) Evaluar la administración de los sistemas de información que soportan las actividades operativas y administrativas.
d) Verificar la efectividad y eficiencia de las operaciones de los sistemas de información desarrollados e implementados en la institución.
e) Verificar el cumplimiento de recomendaciones de auditorías practicadas por la Corte de Cuentas de la República y los resultados de la auditoría interna y externa, relacionados con las Tecnologías de Información y Comunicación.

3.3 Alcance de la Auditoría

Nuestro trabajo consistió en realizar Auditoría de Gestión a las Tecnologías de Información y Comunicación de la Procuraduría para la Defensa de los Derechos Humanos, por el período del 1 de enero de 2013 al 31 de agosto 2015, examinando el uso de los recursos tecnológicos, confidencialidad, confiabilidad, integridad, disponibilidad de la información procesada por los sistemas de información automatizados y apoyo en la automatización de los procesos operativos y administrativos de la PDDH.

La auditoría fue realizada de conformidad a las Normas y Políticas Internas de Auditoría Gubernamental, emitidas por la Corte de Cuentas de la República.

4. PRINCIPALES REALIZACIONES Y LOGROS

En el proceso de la auditoría se identificaron los siguientes logros Institucionales relacionados a la gestión de las TIC durante el período comprendido del 1 de enero de 2013 al 31 de agosto de 2015:

Año 2013
La Procuraduría para la Defensa de los Derechos Humanos contrató consultoría para la elaboración de la hoja de ruta para el diseño, desarrollo y puesta en marcha del "Sistema Informático de Gestión Integral de la PDDH" en el mes de diciembre de 2013.

Año 2014
La Procuraduría para la Defensa de los Derechos Humanos contrató consultoría para la asesoría técnica, acompañamiento y organización de la información necesaria para la elaboración de los requerimientos técnicos del "Sistema Informático de Gestión Integral de la PDDH, en el mes de diciembre 2014.

5. RESULTADOS DE LA AUDITORÍA

5.1 Sistemas Informáticos de Apoyo a los Procesos Sustantivos de la PDDH

5.1.1 Hallazgos de Auditoría

Hallazgo No. 1

PÉRDIDA DE INFORMACIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS

Comprobamos que en fecha 2 de marzo de 2015, se originó una falla en el servidor de correos institucionales de la PDDH, ocasionando la suspensión del servicio y la pérdida total de información de aproximadamente 445 cuentas de usuarios de correo electrónico institucional de todas las dependencias de la entidad, no logrando efectuar la recuperación de la información institucional de los usuarios de sus cuentas de correo.

El Reglamento para el Uso y Control de Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

Continuidad de las operaciones
"Art. Art. 40. El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante períodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares."

El Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el Diario Oficial No. 85, Tomo 399, de fecha 13 de mayo de 2013, establece lo siguiente:

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

Art.35. Son funciones de este Departamento, las siguientes:
"...8) Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional."

La condición se debe a que el Coordinador del Departamento de Informática de la PDDH no efectuó pruebas de la configuración para contingencia basada en un arreglo de discos RAID, para garantizar que toda la información se encontrara respaldada en las dos unidades de disco del servidor de correo, así como también por la obsolescencia de la plataforma de servidores y la falta de un servidor de respaldo para garantizar la continuidad de los servicios de correo electrónico en caso de falla y la falta de planificación en el uso y crecimiento de la información de correo electrónico institucional, respecto a la capacidad instalada de los equipos.

Lo anterior ocasiono la pérdida de información de 445 cuentas de usuarios de correo electrónico institucional, así como el colapso del servidor y la operatividad del servicio de correos Institucional, sin haber tenido la posibilidad de recuperar la información institucional de dichas cuentas, lo cual impactó negativamente el quehacer de los funcionarios y empleados de la oficina central, delegaciones departamentales y locales a nivel nacional, debido a la pérdida de información histórica, comunicaciones y contactos estratégicos relacionados a la defensa de los derechos humanos a nivel nacional.

COMENTARIOS DE LA ADMINISTRACIÓN

En nota de fecha 16 de diciembre de 2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "Al respecto de la configuración del equipo que contiene el correo electrónico institucional, tal y como se detalla en el informe enviado a la Secretaría General y del cual se ha remitido copia, al realizar un arreglo de tipo RAID, es una función de la controladora establecer el estado de funcionamiento del mismo, como prueba de funcionamiento. En tal sentido, no son necesarias pruebas adicionales a la mencionada, en tanto la controladora es la encargada de establecer si existe concordancia entre un disco y el otro, lo cual es el funcionamiento estándar de cualquier dispositivo RAID por diseño.

En este caso particular, la falla no fue detectada debido a que el dispositivo reporta un funcionamiento normal del arreglo, lo cual fue considerado prueba del funcionamiento del mismo y en efecto la falla se detectó únicamente de forma posterior al análisis realizado al servidor y con conocimiento previo de la falla, por lo que no era posible establecer con anterioridad la necesidad de realizar más de una prueba del arreglo referido. Se anexan nuevamente copias de las imágenes de la utilidad de gestión del RAID utilizado en el servidor que demuestran este punto."

COMENTARIO DE LOS AUDITORES

No obstante los comentarios proporcionados por el Coordinador de Informática, sobre la configuración de discos que debía garantizar la continuidad de los servicios en caso de fallo en una de las unidades, y en la que expresa que al realizar un arreglo de tipo RAID, es una función de la controladora establecer el estado de funcionamiento del mismo, y que en tal sentido, no son necesarias pruebas adicionales a la mencionada, se comprobó que previo a la falla, no se garantizó la confiabilidad de la operatividad del servicio de correo institucional a través de pruebas de contingencia y restauración o restablecimiento de Backups de los dispositivos, servidores y sus arreglos en discos, por lo que a la fecha no se ha logrado

recuperar la información de las 445 cuentas de correo electrónico Institucionales, comprobando que con dicha pérdida fueron afectados los usuarios de la PDDH a nivel Nacional, ya que la información era utilizada para consultas históricas y de referencia en casos relacionados con la defensa de los derechos humanos por parte de las Delegaciones Departamentales y Locales; al mismo tiempo, la falta de confiabilidad sobre las operaciones en el correo institucional, conllevó a que se utilicen cuentas de correo públicas y sin garantía de confidencialidad de la información de carácter institucional, por lo tanto el hallazgo se mantiene.

Hallazgo No. 2

SISTEMA INFORMÁTICO INTEGRADO DE GESTIÓN (SIIG) QUE APOYA A LOS PROCESOS SUSTANTIVOS DE LA PDDH ES INEFICIENTE E INEFECTIVO

Verificamos que el Sistema Informático Integrado de Gestión (SIIG) que apoya a los procesos sustantivos de la PDDH es inefectivo e ineficiente, debido a lo siguiente:

a) El sistema SIIG no apoya a todos los procesos sustantivos que realiza la PDDH en función del proceso de la defensa para los derechos humanos, debido a que únicamente se registran las acciones de los procesos de toma de denuncia y orientación, dejando por fuera el registro de la asistencia y acompañamiento, monitoreo de privados de libertad, acciones de prevención para la defensa de los derechos humanos, resoluciones efectuadas por los Delegados Locales y Departamentales, entre otros.

b) El sistema SIIG no cubre las necesidades de información reales de la PDDH, debido a que las opciones de registro de los módulos para toma de denuncia y orientación no se apegan a la realidad de los procesos actuales.

c) La información de los expedientes de tomas de denuncia y otras acciones no se almacenan de forma completa, efectuando la digitalizando de forma parcial, por lo que algunas diligencias o acciones evidenciadas en los expedientes físicos no se respaldan de forma digital.

d) La operatividad del sistema SIIG en relación a los tiempos de respuesta es ineficiente debido a lentitud en el procesamiento y consulta, afectando la atención de los usuarios o víctimas de abuso de los derechos humanos que se acercan a la institución a solicitar ayuda.

e) La seguridad de acceso al sistema por medio de la contraseña de acceso de ingreso (log in de usuario) y su contraseña no es confiable, ya que la entidad no cuenta con una política en la administración de cambio periódico de contraseñas para los usuarios del sistema, además las contraseñas utilizadas son las que inicialmente se asignaron a los usuarios desde la puesta en marcha del sistema en el año 2006.

f) Adicional a las bandejas originales en el sistema SIIG para el alojamiento de los expedientes de los usuarios, se han creado bandejas denominadas "experimentales", en las cuales se están almacenando los expedientes del sistema y archivos digitalizados.

g) Existe inconsistencia en la información de las resoluciones de denuncias que se registran en el sistema SIIG, debido a que únicamente se permite que las resoluciones sean las efectuadas por parte del Procurador General, aunque se ha autorizado a los Delegados

regionales, Departamentales y Locales para poder emitir dichas resoluciones a nivel nacional, las cuales no se pueden registrar en el sistema, por lo que el sistema no dispone de información real y confiable para la toma de decisiones, que para el caso en particular, no reflejaría la cantidad de resoluciones que la PDDH ha efectuado sobre las denuncias a nivel nacional.

El Reglamento para el Uso y Control de Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

"Art. 15. La Unidad de TIC implementará la metodología para el ciclo de vida del desarrollo de sistemas, asegurando que los sistemas de información sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajuste al cumplimiento de las leyes, reglamentos y normativa vigente que les sean aplicables y considerar además lo siguiente:

a) Se deberá priorizar y fomentar el desarrollo de los sistemas de información con recursos internos de la entidad.

b) Definir una adecuada separación de las funciones en los ambientes de desarrollo y producción.

c) Procedimientos de actualización en los manuales de usuario y técnico, para el uso de los sistema en producción y que se encuentra documentado el Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del mismo."

Seguridad de la Información
"Art. 26. La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal."

La condición se debe a que el Coordinador de Informática no ejerce gobernabilidad de las TIC´s (Gobernabilidad de TIC, es la alineación de las Tecnologías de la Información y la Comunicación (TI) con la estrategia del negocio, alineando con las metas y la estrategia a todos los departamentos de la entidad, proporcionando el mejor uso de la tecnología y de sus estructuras organizativas para alcanzarlas) en la Institución, específicamente en lo relacionado al desarrollo de sistemas en apoyo a los procesos sustantivos para la defensa de los derechos humanos; evidenciando además que no se ha involucrado activamente a los usuarios del sistema SIIG durante el proceso de desarrollo ni implementación, por lo que dicho sistema no garantiza proveer los requerimientos de información de cada una de las unidades usuarias.

Lo anterior ocasiona que el Departamento de Informática de la PDDH no pueda garantizar un avance tecnológico acorde a las necesidades de información de la Institución y de la ciudadanía que demanda servicios en pro de la defensa de sus derechos humanos, colocando en riesgo la eficiencia y efectividad de sus procesos sustantivos y administrativos y por ende el registro de información confiable y oportuna para la toma de decisiones, en los procesos relacionados a la defensa de los derechos humanos, generando inconsistencias de integridad de la información en las denuncias ingresadas a las bases de datos del sistema, ocasionando

que la PDDH no cuente con información en sus bases de datos que sirva de apoyo a la toma de decisiones.

COMENTARIO DE LA ADMINISTRACIÓN

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "Sobre estos hallazgos se ha planificado un cronograma de actividades a fin de superar las deficiencias importantes y de impacto. Para ello se planea formar un equipo de desarrollo de Sistemas con estudiantes de Horas sociales para sustentar estas gestiones se anexa copia de memorando REF 155-2015 remitido al Departamento de Recursos Humanos para oficializar esta gestión y permitir la incorporación de estos estudiantes desarrolladores y hacer labores para mejorar el sitio web y algunos de los sistemas de apoyo. También se anexa copia de cartas remitidas por la Universidad Don Bosco solicitando el apoyo.

No se omite manifestar que esta metodología con horas sociales se continuará realizando para avanzar en los proyectos de esta área"

COMENTARIO DE LOS AUDITORES

Debido a que en el Sistema Informático de Gestión Institucional (SIIG) se mantienen aún las condiciones de falta de confiabilidad, indisponibilidad y que no cubre actualmente las necesidades de información que demandan los procesos actuales en materia de Defensa de Derechos Humanos, la condición planteada en el presente hallazgo se mantiene, ya que pese a que existe un diagnóstico para la implementación de una nueva plataforma tecnológica, aún no se garantiza fechas para la implementación y funcionamiento del mismo.

Hallazgo No. 3

FALTA DE CONFIABILIDAD DE LAS BASES DE DATOS DE LA PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS PDDH

Comprobamos que las bases de datos del Sistema Informático Integrado de Gestión (SIIG), Sistema de Información y Gestión de la Procuraduría (SIGEP) y Sistema de Información de Privados de Libertad, para el apoyo a los procesos sustantivos de la PDDH no son confiables, debido a vulnerabilidades de seguridad física y lógica e integridad en la información de las bases, de acuerdo a los siguientes aspectos:

a) La base de datos del Sistema Informático Integrado de Información (SIIG) de la PDDH no es confiable, debido entre otros aspectos a lo siguiente:

   i. La información contenida en los expedientes por denuncias u otras acciones relacionadas con la defensa de los derechos humanos no se almacenan completamente en la base de datos, cargando únicamente información parcial o mínima, para referencia de las diligencias o acciones contenida en los expedientes físicos.

   ii. Las resoluciones a denuncias efectuadas en el sistema por parte de los delegados departamentales o locales no se registran en el sistema como tal, por lo que en la base de datos no se refleja el dato exacto de las resoluciones efectuadas a nivel nacional, sino únicamente las efectuadas por el Procurador General.

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

iii. La información del sistema SIGEP no fue migrada a la base de datos del SIIG, por lo tanto, la base de datos del mismo no cuenta con la información de 88,758 expedientes que incluye denuncias, orientaciones y gestiones de buenos oficios, recibidas y realizadas en cada delegación a nivel nacional, del período 1996 hasta el 2006.

iv. El acceso y carga de la información de expedientes en la base de datos es lenta, sobrepasando los límites de tiempos razonables para el almacenamiento o búsqueda de los mismos.

v. No se evidenció la existencia de un diccionario de datos para la base del SIIG.

b) Verificamos que la base de datos del SIGEP no es confiable debido entre otros aspectos a lo siguiente:

i. La base de datos del sistema SIGEP se encuentra almacenada en un equipo estacionario en la Unidad de Control de Procedimientos, el cual no cuenta con medidas de seguridad físicas ni lógicas para el resguardo de la información, que minimice el riesgo de hurto, daño o pérdida de información ejecutada por personal no autorizado, o desastres naturales.

ii. No existen huellas de auditoría para el rastreo y registro de las actividades de los usuarios del sistema, sobre modificación, adición y eliminación de los registros de la base de datos del sistema SIGEP.

c) Comprobamos que el registro de las personas privadas de libertad del Departamento de Verificación Penitenciaria de la PDDH, no es confiable, debido entre otros aspectos a lo siguiente:

i. El Departamento de Verificación Penitenciaria no cuenta con un sistema y base de datos para el registro centralizado de personas privadas de libertad y de centros autorizados de detención, que cuente con las medidas de seguridad que minimicen el riesgo de hurto, daño o pérdida de información ejecutada por personal no autorizado o desastres naturales.

ii. Los datos con que cuenta la PDDH no garantizan que la información del registro de detenidos que a diario se ingresa, esté actualizada conforme a los datos o notificaciones que se remiten por escrito por las diferentes sedes policiales a nivel nacional, limitando la disponibilidad de información concerniente al tema de privados de libertad y poder dar expedita respuesta a las denuncias sobre personas desaparecidas o sobre la información actualizada de los detenidos en las bartolinas policiales a nivel nacional.

El Reglamento para el Uso y Control de Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

"Art. 15. La Unidad de TIC implementará la metodología para el ciclo de vida del desarrollo de sistemas, asegurando que los sistemas de información sean eficaces, seguros, íntegros,

eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajuste al cumplimiento de las leyes, reglamentos y normativa vigente que les sean aplicables y considerar además lo siguiente:

a) Se deberá priorizar y fomentar el desarrollo de los sistemas de información con recursos internos de la entidad.
b) Definir una adecuada separación de las funciones en los ambientes de desarrollo y producción.
c) Procedimientos de actualización en los manuales de usuario y técnico, para el uso de los sistema en producción y que se encuentra documentado el Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del mismo."

Seguridad de la Información.

"Art. 26. La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal."

Continuidad de las operaciones

"Art. Art. 40. El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante períodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares."

El Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el Diario Oficial no. 85, Tomo 399, de fecha 13 de mayo de 2013, establece lo siguiente:

Sección Cuarta. Del Departamento de Informática.

"Art.35. Son funciones de este Departamento, las siguientes:

1. Proponer al Procurador o Procuradora los sistemas de información electrónica de la Institución, a efecto de satisfacer las necesidades de procesamiento de información y datos, así como su distribución y control.

2. Realizar las copias de respaldo necesarias de los sistemas de almacenamiento de información electrónica de la Procuraduría..."

"...8. Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional..."

La condición se debe a que el Coordinador de Informática, no ha implementado las estrategias o procedimientos que garanticen la confiabilidad en el registro completo de los expedientes en los Sistemas de Información Institucionales y sus bases de datos, con el fin de garantizar que

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

cada denuncia sobre derechos humanos se registre en su totalidad así como el proceso, acciones y/o resoluciones.

La deficiencia ocasiona que el Coordinador de Informática de la PDDH no se garantiza la confiabilidad de la información de las bases de datos, generando lo siguiente:

a) Que la base de datos no refleja el dato exacto de las resoluciones efectuadas a nivel nacional, sino únicamente las efectuadas por el titular (Procurador).

b) Vulnerabilidad por riesgo de pérdida total de la información registrada a la fecha de 88,758 expedientes de las denuncias efectuadas en los períodos de 1996 al 2006 en el sistema SIGEP, el cual además no se encuentra migrada a la base de datos del Sistema SIIG.

c) Uso simultaneo de las bandejas originales o personales del sistema y bandejas experimentales.

d) Pérdida de información de las bases de datos de las personas privadas de libertad de la PDDH, en fecha 30 de mayo de 2013, contenida en el equipo (registro de activo fijo PDDH-Q201B715) que a la fecha no ha sido recuperada ni incorporada a los registros que actualmente alimenta el Departamento de Verificación Penitenciaria en una hoja de cálculo de Excel.

COMENTARIO DE LA ADMINISTRACIÓN

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "Sobre estos hallazgos se ha planificado un cronograma de actividades a fin de superar las deficiencias importantes y de impacto. Para ello se planea formar un equipo de desarrollo de Sistemas con estudiantes de Horas sociales para sustentar estas gestiones se anexa copia de memorando REF 155-2015 remitido al Departamento de Recursos Humanos para oficializar esta gestión y permitir la incorporación de estos estudiantes desarrolladores y hacer labores para mejorar el sitio web y algunos de los sistemas de apoyo. También se anexa copia de cartas remitidas por la Universidad Don Bosco solicitando el apoyo.
No se omite manifestar que esta metodología con horas sociales se continuará realizando para avanzar en los proyectos de esta área."

COMENTARIO DE LOS AUDITORES

No obstante que el Coordinador del Departamento de Informática hace mención de que se ha elaborado un cronograma de actividades a fin de superar las deficiencias importantes y de impacto formando un equipo de desarrollo de Sistemas con estudiantes de horas sociales, y de la inversión por parte de la PDDH en consultorías en las que se concluye sobre el reemplazo y mejora de los procesos y sistemas de apoyo Institucionales, la situación actual de las bases de datos y sistemas de información de la PDDH no es confiable y mantiene un riesgo de pérdida de la información, que para el caso de la información penitenciaria se materializó dicha pérdida por a falta de controles y seguridad de la información en la plataforma tecnológica de la PDDH, por lo que el hallazgo se mantiene.

5.1.2 Conclusión

En la Procuraduría para la Defensa de los Derechos Humanos, el uso de las Tecnologías de Información y Comunicación se constituye en un factor determinante, para el apoyo a sus procesos sustantivos y el cumplimiento de sus objetivos institucionales; sin embargo, a pesar de las inversiones que se han realizado en materia de tecnología de información, no se ha logrado impulsar el desarrollo de un sistema informático para apoyar a los procesos sustantivos de la entidad y que cubra las necesidades de información que en la actualidad demanda la institución, así como la prestación de servicios eficientes y efectivos para los ciudadanos que denuncian violaciones a sus derechos humanos. Esto ha inducido a que las unidades operativas de la PDDH se apoyen con herramientas de ofimática, para cubrir sus necesidades de automatización de procesos, manteniendo un riesgo de pérdida de información y falta de seguridad sobre la información que procesan, por otro lado, se cuenta con un sistema de correo electrónico no confiable e ineficiente para la comunicación institucional, por lo que los funcionarios hacen uso de servicios de correos electrónicos gratuitos y públicos en el cual almacenan y realizar la comunicación institucional, por lo que la Procuraduría para la Defensa de los Derechos Humanos mantiene un riesgo de falta de confiabilidad en la operatividad de los sistemas de información, así como limitantes para garantizar la disponibilidad, continuidad y seguridad de los servicios informáticos de misión crítica y la información de sus bases de datos.

5.2 Infraestructura de Servidores y Seguridad de Plataforma.

5.2.1 Hallazgos de Auditoría

Hallazgo No. 1

FALTA DE CONFIABILIDAD Y OBSOLESCENCIA DE LA PLATAFORMA TECNOLÓGICA DE LOS SERVIDORES CENTRALES QUE SOPORTAN LAS ACTIVIDADES DE PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN DE LOS SISTEMAS

Comprobamos que existe obsolescencia en la plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de la información de los sistemas de apoyo a los procesos sustantivos y administrativos, así como los servicios informáticos, comunicaciones y seguridad de la red de la Procuraduría para la Defensa de los Derechos Humanos.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

Art. 7. El Plan Estratégico de TIC debe:

"...c) Contemplar el presupuesto operacional y de inversiones, las estrategias de suministro y de adquisición (contratación de servicios y adquisición de equipos) y los requisitos legales..."

Capítulo IV. Proyectos de Tecnologías de Información.

Art. 13. "La Unidad de TIC, efectuará diagnóstico de las necesidades y requerimientos tecnológicos de las dependencias de la Entidad y deberá proyectar las mejoras de las

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

tecnologías de información y comunicaciones, considerando los costos de transición, viabilidad, capacidad técnica, instalaciones, riesgos tecnológicos, vida útil y tasas de crecimiento de la infraestructura tecnológica."

El Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el Diario Oficial No. 85, tomo 399, de fecha 13 de mayo de 2013, establece lo siguiente:

Sección Cuarta. Del Departamento de Informática

Art. 35.Son funciones de este Departamento, las siguientes:

"...8) Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional."

La causa del hecho es debido a que el Coordinador de Informática no gestionó ante la superioridad que fuesen incluidos en los presupuestos ni en los planes de trabajo de los años auditados, la actualización e implementación de una nueva plataforma tecnológica de los servidores centrales que soportan las actividades de procesamiento y almacenamiento de información de los sistemas, así como la falta de espacio para almacenamiento y la frecuente pérdida de información.

Al no tener un presupuesto acorde a las necesidades para la tecnología de información y comunicación ni establecer en sus planes de trabajo dichas acciones, no se puede contar con las estrategias de suministros y adquisición de nuevos equipos y contratación de servicios, lo que permite poca capacidad de innovación ya que no se logra incrementar sistemas, procesos o capacidades puesto que los equipos no son suficientemente robustos, lo que implica un alto riesgo de interrupción/colapso de los servicios informáticos que ofrece el Departamento de Informática, por lo que se mantiene el riesgo de no asegurar la continuidad y restablecimiento de la operatividad de los sistemas, debido a la obsolescencia tecnológica.

COMENTARIOS DE LA ADMINISTRACION

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "En relación a este hallazgo se anexa copia del Memorándum con referencia INF150-2015 en el cual se puede constatar la Solicitud de Compra por parte del Departamento de Informática de dos servidores con las siguientes características.
Servidor para Rack Un (1) procesador Xeon de 8 Cores instalado, soporte para 2 procesadores máximo*
Dos (2) bancos de 32 GB de memoria RAM (64 en total)
Cuatro (4) Discos Duros SAS 300GB 10,000 RPM, intercambiables en caliente (especificar cantidad de bahías adicionales si posee)
Controladora RAID SAS (2) puertos de red de 1Gbps, como mínimo
Entre 1 y 2 unidades de espacio en rack (especificar)
Controladora de administración de sistema que permita extracción de logs, actualización de firmware de componentes del sistema, visualización de pantalla del servidor, encendido remoto del servidor como mínimo.
100% de compatibilidad con sistemas de virtualización HYPER-V, XenServer o KVM (especificar características de compatibilidad y/o certificaciones)

Compatible con Windows Server 2012 R2 y Red Hat Enterprise Linux como mínimo
Licencia de Windows Server 2012 R2 Standard OLP NL GOV, 2 Procesadores
Fuente de alimentación redundante
Incluir hardware para instalación en rack; incluir instalación, configuración y puesta en marcha de virtualización y Directorio Activo.
3 años de garantía
* Podría ser también dos procesadores instalados de 4 cores, pero es menos deseable.

Además para evidenciar no solo la gestión de solicitud sino también la continuidad en el proceso, se anexa también memorándum con referencia INF154-2015, en el cual el Departamento de Informática remite a UACI la evaluación a las ofertas presentadas por proveedores que participaron en la Libre Gestión No. 341/2015 referente al "Suministro de equipo Informático (Equipos de protección perimetral, servidores y Access point) y licencias de software antivirus".
Consideramos que con estas acciones el Departamento de Informática está en la ruta de actualización de su plataforma tecnológica de los servidores centrales a fin de soportar las actividades y servicios previstos. Lo que también se comprueba con las nuevas características y capacidades de estos servidores que se espera adquirir."

COMENTARIOS DE LOS AUDITORES

En relación a los comentarios efectuados por el coordinador del Departamento de Informática, se han identificado acciones por parte de la PDDH enfocadas mejorar la plataforma tecnológica de servidores institucionales, haciendo mención sobre las ofertas presentadas por proveedores que participaron en la Libre Gestión No. 341/2015 referente al "Suministro de equipo Informático (Equipos de protección perimetral, servidores y Access point) y licencias de software antivirus"; no obstante la PDDH se encuentra en proceso de adquisición de dichos servidores, la operatividad de los sistemas a través de los servidores actuales se mantiene en riesgo y aún no se garantiza el tiempo que transcurrirá para que la PDDH adquiera, instale e implemente en ellos los servicios de TIC. Por lo tanto, la deficiencia no se da por superada.

Hallazgo No. 2

CARENCIA DE APROBACION DEL PLAN DE CONTINGENCIA POR LA MAXIMA AUTORIDAD

Comprobamos que el Departamento de Informática de la PDDH no cuenta con un plan de contingencia aprobado por la Máxima Autoridad.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

"Art.39. La Unidad de TIC, deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad, este plan debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la Entidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas, este plan debe probarse y actualizarse

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

atendiendo la realidad tecnológica de la entidad al menos una vez al año. Deberá ser comunicado a los niveles pertinentes."

El Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el Diario Oficial No. 85, tomo 399, de fecha 13 de mayo de 2013, establece lo siguiente:

SECCIÓN CUARTA. DEL DEPARTAMENTO DE INFORMÁTICA

Art. 35.Son funciones de este Departamento, las siguientes:

"...8) Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional."

El hecho obedece a que el Coordinador del Departamento de Informática no ha elaborado las políticas para el desarrollo de contingencias contra desastres naturales o provocados por el hombre.

El no tener un plan de contingencia, permite que en un momento determinado no se tenga un plan que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos necesarios para la mitigación de un siniestro (Terremotos, corte de energía eléctrica, inundaciones, entre otros), por lo cual existe vulnerabilidad y riesgos que amenazan la plataforma tecnológica de TIC y estas afectan de forma parcial o total la operatividad de los servicios de la Entidad.

COMENTARIOS DE LA ADMINISTRACION

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "Sobre este hallazgo se anexa copia del Memorándum con referencia INF156-2015 en el cual el Departamento de Informática, remite al Departamento de Planificación el borrador de la primera versión del "Plan de Contingencia y continuidad de operaciones", y del cual se prevé su aprobación para el año 2016..."

COMENTARIOS DE LOS AUDITORES

Debido a que la Procuraduría para la Defensa de los Derechos Humanos aún no cuenta con un plan de Contingencia de TIC aprobado por la máxima autoridad, ni con pruebas de dicho Plan y los resultados documentados de las acciones de contingencia a ejecutar ante un evento que paralice parcial o totalmente los servicios TIC institucionales, la observación se mantiene.

Hallazgo No. 3

VULNERABILIDADES EN LA SEGURIDAD DE LA SALA DE RESGUARDO DE SERVIDORES CENTRALES INSTALADOS EN EL DEPARTAMENTO DE INFORMÁTICA

Comprobamos que existe vulnerabilidad en la seguridad física de la sala de resguardo de los servidores centrales institucionales instalados en el Departamento de Informática de la PDDH, los cuales proveen de los servicios informáticos (Sistemas administrativos y de apoyo a los procesos sustantivos, base de datos, página Web, correo electrónico institucional, sistemas de

seguridad perimetral, entre otros) a los usuarios de la red tanto en la oficina central como en las delegaciones departamentales y locales. A continuación se detallan algunas de ellas, las cuales representan riesgos de acceso físico y desastres naturales:

a) Vulnerabilidad en el acceso físico al Área de Servidores o el Data Center, ya que no cuenta con un área específica para su alojamiento y resguardo, compartiendo actualmente el área utilizada por técnicos de informática.
b) Las áreas de acceso no se encuentran restringidas, no poseen puertas con chapas electrónicas o biométricas para el control del ingreso del personal.
c) No existen las medidas para el monitoreo de la seguridad (cámaras de video vigilancia, alarmas, detectores de humo, medidores de temperatura, medidores de humedad, entre otros).
d) La infraestructura de servidores y rack de comunicaciones no se encuentran instalados sobre un piso falso o tarimas especiales que minimicen el riesgo de daños a los equipos en caso de terremotos, inundaciones o fugas de agua internamente, ya que se encuentran instalados en el mismo nivel del baño dentro de la Jefatura del Departamento de Informática.
e) Cielos falsos sobre la ubicación de los gabinetes de servidores y rack de comunicaciones con señales de filtración de agua así como en el piso.
f) En el área de servidores se encuentra resguardado equipo de cómputo inservible o por reparar, el cual puede servir de refugio y crianza de roedores u otro tipo de plagas, los cuales pueden dañar dichos servidores.
g) Conexiones de cables eléctricos y cable estructurado (UTP) en desorden, exponiendo a los equipos a daños por alzas o bajas de la potencia eléctrica.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

Art.27. "La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, Switch y otros dispositivos."

El Reglamento de Organización y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, publicado en el D.O. No. 85, tomo 399, de fecha 13 de mayo de 2013, en su Art.35, numeral 8, en las funciones del Departamento de Informática, expresa lo siguiente: "8) Proponer planes y políticas de seguridad para el almacenamiento, utilización, transmisión y disposición final de la información electrónica y de la infraestructura tecnológica institucional."

La causa obedece a falta de gestión por parte del Coordinador del Departamento de Informática, al no implementar políticas de seguridad para autenticar y autorizar el acceso a los sistemas de información operativos y bases de datos, así como para garantizar la seguridad para el almacenamiento, utilización, disposición de la información y la infraestructura tecnológica.

Dicha condición ocasiona que exista un alto riesgo que la información sensible que maneja los servidores de la PDDH se pierda o destruya, por no existir restricciones a personal no

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

autorizado para el acceso al cuarto de servidores, ya que la información que se resguarda no se encuentran en cajas de seguridad y se encuentra en lugares de acceso al personal del área.

COMENTARIOS DE LA ADMINISTRACION

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "De igual forma el Departamento de Informática, ya ha realizado acciones para superar las vulnerabilidades y estado de la sala de resguardo de servidores centrales, para sustentar esta afirmación se anexa copia del memorando con referencia INF147-2015 en el cual el Departamento de Informática, explica a los diferentes Departamentos de la Procuraduría para la Defensa de los Derechos Humanos, del proceso de Mantenimiento a los equipos alojados en la sala en cuestión labores planificadas y registradas en PAT 2015, además se aprovechó la ocasión para coordinar con la Unidad de Mantenimiento a fin de aprovechar la suspensión de servicios y apagado de servidores, para hacer un cambio total de cielo falso y dar mantenimiento a los Aires acondicionados de estas oficinas. De igual forma se dio mantenimiento a los equipos ubicados en el edificio AMSA para lo cual se anexa memorando que hace referencia a este servicio."

COMENTARIOS DE LOS AUDITORES

De acuerdo a los comentarios del Coordinador del Departamento de Informática se manifiesta que se han realizado gestiones para subsanar las observaciones planteadas, así como la ejecución de acciones, como el cambio de cielos falsos y mantenimiento a aires acondicionados en la sala de resguardo de los servidores, no obstante, las condiciones de vulnerabilidad a la seguridad física por el acceso no autorizado al área y medidas para alertar o minimizar los riesgos de seguridad de la información que se administra en los servidores, aún persisten, por lo que la observación se mantiene.

5.2.2 Conclusión

La Procuraduría para la Defensa de los Derechos Humanos cuenta con una plataforma de hardware, software y comunicaciones administrada por el Departamento de Informática para proporcionar soporte técnico a los requerimientos de las diferentes Unidades Organizativas, usuarias de los servicios informáticos y sistemas de información, servidores institucionales, bases de datos y redes de comunicación a nivel nacional. Así mismo la seguridad lógica de la red se encuentra basada en un firewall para filtrar los accesos entrantes y/o salientes, para garantizar la seguridad en el uso del Internet y programas utilizados para las diferentes labores de los usuarios; no obstante, no se cuenta con protección de virus, antimalware, bloqueo de spam y control de dispositivos (USB, unidades ópticas, dispositivos de imagen, dispositivos bluetooth, Modem, lector de tarjetas inteligentes, entre otros).

A pesar de que existe un apoyo constante, por parte del Departamento de Informática para dar soporte a los procesos sustantivos de la PDDH, el riesgo de que ocurra una interrupción prolongada de los servicios de tecnología de información y comunicación es alto, debido a la obsolescencia de los servidores institucionales y que no se cuenta con un plan de contingencia que garantice la continuidad de los servicios.

CORTE DE CUENTAS DE LA REPÚBLICA

5.3 Planificación y Organización de las TIC´S.

5.3.1 Hallazgos de Auditoría

Hallazgo No. 1

FALTA DE SEGUIMIENTO A CONTRATACIÓN DE SERVICIOS DE INTERNET PARA GARANTIZAR LA EFICACIA DEL SERVICIO PRESTADO

Comprobamos que durante el período comprendido del 1 de julio al 31 de diciembre de 2013, se contrató servicios de ´Internet Dedicado´ a través del Contrato No. 017/2013, de fecha 28 de junio de 2013 para los cuatro edificios de San Salvador, 13 delegaciones Departamentales y 4 delegaciones locales de la PDDH, según el siguiente detalle:

Ubicación de Edificio	Descripción del Servicio
Edificio AMSA	1Mbps y otro de 2mbps
Edificio de Tutela	8Mbps y otro de 2mbps
Edificio 444	1Mbps
Escuela de Derechos Humanos	1Mbps
Delegaciones Departamentales	1Mbps
Delegación de San Miguel	256kbps
Delegaciones de la Paz, Soyapango, Cuscatlán	512kbps
Demás delegaciones	512kbps

Además, para el período del 1 de marzo de 2014 al 31 de diciembre de 2014, según Contrato No.019/2014 de fecha 28 de febrero de 2014, la contratación y la descripción del mismo servicio se mantuvo igual; sin embargo, al realizar visitas a las oficinas regionales de la PDDH en los municipios de Santa Tecla, Santa Ana, Ahuachapán, Cojutepeque, San Vicente, Zacatecoluca, Soyapango y Chalatenango, así como a diferentes Unidades Organizativas en oficina central, se verificó que dicho servicio contratado no satisfizo las necesidades de información de los usuarios debido, entre otros, a la limitantes en la carga y actualización de expedientes a las bases de datos del SIIG sobre denuncias, orientaciones y gestiones de buenos oficios recibidas y realizadas en cada delegación departamental y local, así como en la operatividad del sistema que se conectan a los servidores a través de dichos enlaces, correo electrónico institucional y lentitud o indisponibilidad de navegación para la consulta de sitios web.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece en su Art. 27 lo siguiente:

"La Unidad de TIC deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica"

La deficiencia se debe a que no hubo determinación adecuada de requerimientos para la contratación del servicio por parte del Coordinador de Informática, quien fungió como Administrador de Contrato para los períodos observados, en el sentido de definir las características necesarias para satisfacer las necesidades de los usuarios.

La falta de seguimiento por parte del Administrador de Contrato, originó que se prorrogara el contrato con las mismas especificaciones sin que se cumpliera con una recepción adecuada y confiable de información, tomando en cuenta que existió lentitud en el acceso y navegación con lo cual se limita el aprovechamiento del recurso, afectando el cumplimiento de los objetivos para los que fue adquirido el servicio.

COMENTARIOS DE LA ADMINISTRACIÓN

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "En relación a este hallazgo se anexa copia del correo remitido a Claro actual proveedor del servicio de Internet, en el cual se solicita registro del análisis de tráfico de estos servicios prestados en las diferentes oficinas de la PDDH en todo el país, también presenta la copia de la información entregada por Claro.
Con la nuevas funciones técnicas provistas por los equipos de seguridad perimetral y conectividad particularmente con la administración de filtrado de contenido web que permite este equipo, será posible para el Departamento de Informática determinar con precisión el uso adecuado que se esté dando a este recurso (Internet) por parte de los usuarios de la PDDH, contaremos con reportes de consumo entre los que se mencionan: Ancho de banda utilizado, Usuarios que más usan ancho de banda, Servicios más usados, Páginas web más visitadas, Usuarios que más tiempo emplean navegando, Reporte de páginas web empleadas por usuario, Páginas web más filtradas, Usuarios más filtrados, Categorías más filtradas (Todos estos reportes son solicitados en los TDR de adquisición de los equipos)."

COMENTARIOS DE LOS AUDITORES

No obstante los comentarios brindados por el Coordinador del Departamento de Informática la observación se mantiene, debido a que a la fecha el servicio de Internet y enlaces de comunicación mantienen las limitantes identificadas en la observación, y la mejora será implementada hasta que la PDDH adquiera los equipos de seguridad perimetral y conectividad particularmente con la administración de filtrado de contenido web, con lo que, según la entidad, será posible determinar con precisión el uso adecuado que se esté dando a este recurso (Internet) por parte de los usuarios de la PDDH y obtener un mejor rendimiento del servicio.

Hallazgo No. 2

FALTA DE CONTROL DE INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE

Comprobamos que el Departamento de Informática no tiene control sobre los procedimientos de instalación y desinstalación de software en los diferentes equipos informáticos de la PDDH, ya que no existe un detalle específico de los diferentes equipos estacionarios y portátiles (laptops) que detalle cuándo y a cuáles les fueron instalados los softwares que cuenten con sus respectivas licencias extendidas por el fabricante y compradas por la entidad para tal fin o con software libre.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público, emitido por la Corte de Cuentas de la República y publicado en el Diario Oficial No. 125, tomo 404, de fecha 08 de julio de 2014, establece lo siguiente:

Licenciamiento de software.

"Art.45. Todo el software instalado en la entidad, deberá estar amparado con la respectiva licencia extendida por el fabricante, otorgando a la entidad el derecho de instalación y uso de los mismos, de conformidad a lo establecido por la ley".

"Art. 47. La Unidad de TIC es la responsable de la instalación de software libre, debiendo justificar los usuarios las necesidades de su uso".

Causa de dicha observación, obedece a la falta de organización y planificación en llevar un control de instalación y desinstalación de software por parte del Coordinador de Informática.

Como consecuencia de dicha observación, no existe un control sobre la instalación de software, no llevando de esa manera un control exacto de las licencias en operación y el equipo en el cual se encuentra en uso.

COMENTARIOS DE LA ENTIDAD

En nota sin referencia de fecha 9 de diciembre de 2015, en respuesta a nota REF-DA7-954-2015, el coordinador del Departamento de Informática, efectuó los comentarios siguientes: "Similar al hallazgo anterior el Departamento de Informática ha planificado superar estas observaciones con la solicitud de servicio que se establece en los TDR del proceso de Libre Gestión No. 341/2015 referente al "Suministro de equipo Informático (Equipos de protección perimetral, servidores y Access point) y licencias de software antivirus", en el cual se solicita la configuración y ejecución del servicio del Directorio Activo para los equipos servidores.
Lo que técnicamente permitirá poder administrar los servicios, recursos, usuarios, etc. que formen parte del nuevo dominio a configurar."

COMENTARIOS DE LOS AUDITORES

En relación a las respuestas emitidas por el Coordinador de Informática, la observación se mantiene, debido a que aún no se cuenta con las herramientas de software y hardware con las que se tiene previsto subsanar dicha limitante, la cual será subsanada según la entidad a través de la adquisición relacionada con la solicitud de servicio que se establece en los TDR del proceso de Libre Gestión No. 341/2015 referente al "Suministro de equipo Informático (Equipos de protección perimetral, servidores y Access point) y licencias de software antivirus"

5.3.2 Conclusión

La PDDH no cuenta con herramientas tecnológicas administradas por parte del Departamento de Informática Institucional para proporcionar un adecuado soporte técnico a los requerimientos de las diferentes Unidades Organizativas usuarias de las distintas plataformas de servicios informáticos y sistemas de información, servidores institucionales, bases de datos y redes de comunicación y licencias de software a nivel nacional, ya que no cuenta con herramientas administradas concernientes a normas, políticas y procedimientos de seguridad y confiabilidad de los sistemas informáticos para evitar posibles fallos. Por otra parte, las compras analizadas cumplen con las disposiciones legales, técnicas y económicas aplicables.

Teléfonos PBX: (503) 2592-8000, Código Postal 01-107
http: //www.cortedecuentas.gob.sv, 1a. Av. Norte y 13a. C. Pte. San Salvador El Salvador, C.A.

El Departamento de Informática como unidad de apoyo a la consecución de objetivos, necesita fortalecerse en aspectos administrativos sobre cómo formular metas alcanzables en los tiempos programados asegurándose de contar con los recursos necesarios (Recurso humano, disponibilidad de recursos financieros entre otros) ya que al dar cumplimiento oportuno a las actividades fortalece la eficacia en el trabajo y evita solicitar reprogramaciones; otro de los aspectos que deben fortalecerse es el proceso de elaboración, revisión y autorización y divulgación del Marco Normativo Institucional referente a las Tecnologías de Información y Comunicación que ayudará a mejorar la administración de las Tecnologías a nivel Institucional, en el sentido de brindar directrices para el adecuado uso de los Recursos Tecnológicos con los que cuenta la Procuraduría. Asimismo, es necesario fortalecer los controles de aquellos servicios dados en outsoursing a fin de garantizar la calidad de la prestación del servicio conforme a las especificaciones técnicas solicitadas para garantizar la satisfacción de los usuarios de los mismos.

6. ANALISIS DE INFORMES DE AUDITORÍA INTERNA Y DE FIRMAS PRIVADAS

6.1 Informes de Auditoría Interna

Durante el período que comprende nuestra auditoría, la Unidad de Auditoría Interna no emitió informes de auditoría relacionados a las Tecnologías de Información y Comunicación, por lo que no existen hallazgos de auditoría ni recomendaciones que deban ser evaluados.

6.2 Informes de Auditoría de Firmas Privadas

La Administración superior de la PDDH no contrató servicios de auditoría externa durante el período auditado, por lo que no existen observaciones ni recomendaciones relativas a los sistemas informáticos para su respectivo análisis.

7. SEGUIMIENTO A LAS RECOMENDACIONES DE AUDITORÍAS ANTERIORES

Debido a que la presente auditoría es la primera acción de control que realiza la Corte de Cuentas de la República sobre las Tecnologías de Información y Comunicación a la Procuraduría para la Defensa de los Derechos Humanos, y no se identificaron auditorías internas o externas con recomendaciones relacionadas a las Tecnologías de Información y Comunicación, no efectuamos seguimiento a recomendaciones.

8. CONCLUSION GENERAL

Como producto de la Auditoría de Gestión a las Tecnologías de Información y Comunicación a la Procuraduría para la Defensa de los Derechos Humanos, por el período del 1 de enero de 2013 al 31 de agosto de 2015, concluimos en lo siguiente:

La PDDH cuenta con una plataforma tecnológica basada en hardware, software y enlaces de comunicación a nivel nacional, con la cual apoya a los procesos sustantivos y administrativos institucionales. No obstante, existe falta de gobernabilidad de las Tecnologías de Información y Comunicaciones por parte del Departamento de Informática, además la institución no ha sido económica en las inversiones en TIC, debido a que no se han enfocado en generar un valor agregado a la Entidad, ya que los proyectos en TIC no se implementan de forma eficiente y eficaz en apoyo a los procesos sustantivos, por lo tanto, es imperativo que la Institución a través de la alta gerencia determine lineamientos para que exista gobernabilidad de las TIC.

Además, no existe una herramienta para la identificación y administración de los riesgos asociados a las TIC, que minimice el riesgo de interrupciones de los servicios de información y comunicación dentro de la entidad, la pérdida de información institucional almacenada en las bases de datos de los servidores centrales, infección de equipos de la red por ataque de virus malware entre otros y garantice la seguridad física y lógica de los sistemas informáticos. Asimismo, la infraestructura de servidores de la PDDH es ineficiente y no es económica, ya que se encuentra integrada por equipos obsoleto (sin soporte en el mercado y/o desfasado por el fabricante) lo cual mantiene un riesgo de falta de confiabilidad en la operatividad de la infraestructura, así como limitantes para garantizar la continuidad de los servicios de misión crítica de apoyo a los procesos para la defensa de los derechos humanos, como lo es el sistema integrado SIIG y SIGEP, los cuales implican a las bases de datos que contienen la información de denuncias a derechos humanos, desde 1995 al 2015. Existe además vulnerabilidad en la seguridad física de la sala de resguardo de los servidores centrales instalados en la unidad de informática y la estructura organizativa de la unidad de informática no responde a las necesidades de soporte técnico y de desarrollo de proyectos informáticos de la Procuraduría para la Defensa de los Derechos Humanos.

9. RECOMENDACIONES DE AUDITORÍA

Recomendación No. 1

Recomendamos al Procurador para la Defensa de los Derechos Humanos, instruya a la Secretaría General a fin de que en coordinación con el Jefe de la Unidad Financiera Institucional y el Jefe de Informática realicen las gestiones necesarias ante las instancias correspondientes, a fin de que sean establecidos en el Presupuesto Institucional, los recursos necesarios para la actualización de la plataforma tecnológica de la PDDH, para sustituir los equipos que se encuentran en el cuarto de servidores, por equipos que cumplan las características técnicas necesarias para el funcionamiento de los procesos que realiza la Institución.

Recomendación No. 2

Recomendamos al Procurador para la Defensa de los Derechos Humanos, instruya a la Secretaría General a fin de que en coordinación con la Jefatura de Planificación y de Informática, se realicen las gestiones para que se elabore un plan de contingencia de TIC actualizado y que soporte las necesidades reales de infraestructura tecnológica de la PDDH en función de mantener la continuidad de los servicios críticos de TIC y que garantice un restablecimiento y recuperación de los servicios informáticos de manera efectiva, así mismo que dicho plan cuente con las pruebas de su ejecución y con la aprobación de la máxima autoridad de la PDDH.

Recomendación No. 3

Recomendamos al Procurador para la Defensa de los Derechos Humanos instruya a la Secretaría General a fin de que en coordinación con las Jefaturas de Planificación y de Informática, se elaboren políticas y procedimientos para la seguridad física y lógica de la plataforma tecnológica que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así

como sea asignado un espacio con las condiciones mínimas para una infraestructura de cuarto de servidores (Puertas con accesos biométricos, cámaras de seguridad, aire acondicionado, detectores de humo, medidores de temperatura, medidor de humedad, etc.), debiendo tener una ubicación en una área que minimice el riesgo de acceso por personal no autorizado.

10. PÁRRAFO ACLARATORIO

Este informe se refiere a la Auditoría de Gestión a las Tecnologías de Información y Comunicación a la Procuraduría para la Defensa de los Derechos Humanos, por el período del 1 de enero de 2013 al 31 de agosto 2015, la cual fue desarrollada de acuerdo a la Ley de la Corte de Cuentas de la República y las Normas y Políticas de Auditoría Gubernamental, emitidas por la Corte de Cuentas de la República.

San Salvador, 21 de diciembre de 2015.

DIOS UNIÓN LIBERTAD

Dirección de Auditoría Siete