

San Salvador, 04 de marzo de 2021

Miembros de Junta Directiva

Presente

El presente resumen ejecutivo contiene los resultados de la **Auditoría a los Sistemas Informáticos de FOPROLYD al 31 de diciembre de 2020**. La auditoría fue realizada en cumplimiento a los Artículos 30 y 31 de la Ley de la Corte de Cuentas de la República, y a las Normas de Auditoría Interna del Sector Gubernamental emitidas por la Corte de Cuentas de la República.

El presente examen de Auditoría a los Sistemas Informáticos de FOPROLYD se realizó en cumplimiento del **Capítulo IV “Participación de profesionales o especialistas en la actividad de Auditoría”**, artículos del 43 al 50 de las Normas de Auditoría Interna del Sector Gubernamental emitidas por la Corte de Cuentas de la República; y se contó con la Participación de un equipo especialista en Sistemas Informáticos del Departamento de Riesgo Operacional y Tecnológico de la Superintendencia del Sistema Financiero.

En la realización de los procedimientos de auditoría se identificaron 10 deficiencias significativas que reportar y que se encuentran detalladas en el numeral 4 del presente informe.

De acuerdo a los resultados obtenidos, se concluye que los sistemas informáticos y demás recursos tecnológicos de FOPROLYD actualmente no cuentan con los controles internos, administración de riesgos, planificación y organización de recursos, entrega y soporte de servicios, monitoreo y evaluación de los recursos tecnológicos que permitan a FOPROLYD contar con seguridad razonable de los Sistemas Informáticos y demás recursos tecnológicos.



Licenciada Iris Nathaly Melgar Mercado

Jefe Interina y Supervisora de la Unidad de Auditoría Interna



GOBIERNO DE
EL SALVADOR

**FONDO DE PROTECCIÓN DE LISIADOS Y
DISCAPACITADOS A CONSECUENCIA DEL
CONFLICTO ARMADO (FOPROLYD)**

UNIDAD DE AUDITORÍA INTERNA

INFORME DE AUDITORIA N° 01/2020

**AUDITORIA A LOS SISTEMAS INFORMATICOS DE
FOPROLYD**

AL 31 DE DICIEMBRE DE 2020

CONTENIDO

1.	OBJETIVOS	1
1.1	Objetivo General.	1
1.2	Objetivos Específicos.	1
2.	ALCANCE DE LA AUDITORIA.	2
3.	PROCEDIMIENTOS DE AUDITORÍA APLICADOS.	2
4.	RESULTADO DE LA AUDITORIA.	4
5.	SEGUIMIENTO A RECOMENDACIONES CONTENIDAS EN LOS INFORMES DE AUDITORIAS ANTERIORES REALIZADAS POR AUDITORIA INTERNA, CORTE DE CUENTAS Y FIRMAS PRIVADAS.	7
5.1.	AUDITORIA INTERNA.	7
5.2.	AUDITORIA EXTERNA:	18
5.3.	CORTE DE CUENTAS DE LA REPÚBLICA.	19
6	RECOMENDACIONES DE AUDITORIA.	19
7	CONCLUSIÓN.	19
8	PÁRRAFO ACLARATORIO.	20

San Salvador, 04 de marzo de 2021

Miembros de Junta Directiva

Presente

El presente informe contiene los resultados de la **Auditoría a los Sistemas Informáticos de FOPROLYD al 31 de diciembre de 2020**. La auditoría fue realizada en cumplimiento a los Artículos 30 y 31 de la Ley de la Corte de Cuentas de la República, y a las Normas de Auditoría Interna del Sector Gubernamental emitidas por la Corte de Cuentas de la República.

El presente examen de Auditoría a los Sistemas Informáticos de FOPROLYD se realizó en cumplimiento del **Capítulo IV “Participación de profesionales o especialistas en la actividad de Auditoría”**, artículos del 43 al 50 de las Normas de Auditoría Interna del Sector Gubernamental emitidas por la Corte de Cuentas de la República; y se contó con la Participación de un equipo especialista en Sistemas Informáticos del Departamento de Riesgo Operacional y Tecnológico de la Superintendencia del Sistema Financiero.

1. OBJETIVOS

1.1 Objetivo General.

Realizar una evaluación objetiva que permita determinar el correcto funcionamiento y operación de los sistemas y aplicativos informáticos de FOPROLYD, el cumplimiento de la normativa y estándares aplicables al área tecnológica y la adecuada organización y segregación de funciones de la Unidad de Informática.

1.2 Objetivos Específicos.

- 1) Verificar que exista un Plan de Continuidad del Negocio y Plan de Recuperación ante Desastres.
- 2) Evaluar el control interno de la Unidad de Informática que permita obtener un grado de seguridad razonable de las diferentes etapas del ciclo de vida de los sistemas informáticos.

- 3) Comprobar que la Unidad de Informática de FOPROLYD cuente con los instrumentos normativos y la implementación de estándares en el área de tecnologías de información de conformidad a las actividades que realizan.
- 4) Verificar que la Unidad de Informática cuente con los recursos necesarios: financieros, tecnológicos y talento humano, que permita cumplir con los objetivos y metas propuestas y brindar un servicio de calidad.
- 5) Evaluar el control que la Unidad Informática administra sobre los requerimientos y solicitudes de las Unidades de Gestión de FOPROLYD, a fin de garantizar la satisfacción de los usuarios.
- 6) Verificar que los niveles de acceso a los sistemas y aplicativos informáticos, se encuentren de conformidad al perfil de puestos y a las funciones que realizan los usuarios.
- 7) Verificar la apropiada segregación de funciones entre el personal de la Unidad de Informática.
- 8) Brindar seguimiento a la implementación de recomendaciones realizadas en auditorías anteriores.

2. ALCANCE DE LA AUDITORIA.

Realizar un examen de auditoría a los sistemas informáticos de FOPROLYD que comprenda: a) El funcionamiento y operación de los sistemas y aplicativos informáticos, b) El cumplimiento de normativa y estándares aplicables al área tecnológica, y c) La organización y segregación de funciones de la Unidad de Informática. El examen de auditoría se realizará el 31 de diciembre de 2020, y se considerará como marco de referencia las Normas de Auditoría Interna del Sector Gubernamental emitidas por la Corte de Cuentas de la República y estándares internacionales de auditoría a las tecnologías de información.

3. PROCEDIMIENTOS DE AUDITORÍA APLICADOS.

Los procedimientos de auditoría fueron planificados y desarrollados directamente por el equipo especialista en Sistemas Informáticos del Departamento de Riesgo Operacional y

Tecnológico de la Superintendencia del Sistema Financiero; y dentro de los cuales se encuentran:

- a) Entrevistas virtuales con la Unidad de Auditoría Interna y Gerencia General de FOPROLYD.
- b) Entrevistas virtuales con el personal de la Unidad de Informática de FOPROLYD para conocer el control interno aplicable.
- c) Verificación de la siguiente información aplicable a la Unidad de Informática:
 - i. Organigrama de TI y Descripción de las funciones.
 - ii. Descripción de las características de la plataforma tecnológica.
 - iii. Diagrama de red de comunicaciones internas y externas.
 - iv. Portafolio de proyectos tecnológicos desarrollados en los años 2019 y 2020.
 - v. Capacitaciones de la Unidad de Informática en los años 2019 y 2020.
 - vi. Características de la definición de los ambientes de desarrollo, pruebas y producción.
 - vii. Análisis de los procesos, políticas y procedimientos de TI con los que cuenta la institución.
 - viii. Ubicación y características del centro de datos principal y alternativo.
 - ix. Análisis de los procesos definidos como críticos.
 - x. Revisión de: Estrategias y Políticas de continuidad del negocio, Programa de ejecución de pruebas a los planes de continuidad del negocio 2019 y 2020, Análisis de impacto del negocio (BIA), Plan de continuidad del negocio (BCP), Plan de Recuperación de Desastres (DRP).
 - xi. Revisión de la evidencia de las pruebas realizadas al Plan de Continuidad del Negocio.
 - xii. Revisión de Informes de las áreas correspondientes y de Auditoría relacionados con la ejecución de las pruebas a los planes de continuidad.
 - xiii. Verificación de la realización de mantenimientos preventivos de software y hardware del año 2019 y 2020.
 - xiv. revisión de usuarios, roles y perfiles de acceso a los sistemas informáticos y a sus bases de datos.
 - xv. Políticas de seguridad de la información.
 - xvi. Inventario de plataforma tecnológica.

- d) Verificación del Plan de Acción desarrollado para implementar las recomendaciones resultantes de informes de auditoría realizados al área de TI de la entidad.

4. RESULTADO DE LA AUDITORIA.

Al efectuar los procedimientos de Auditoria a los Sistemas Informáticos de FOPROLYD se identificaron las siguientes observaciones:

4.1. FOPROLYD no cuenta con un Sistema de Gestión de Continuidad del Negocio, que incluya como mínimo los siguientes aspectos:

- a) Una política de continuidad del negocio;
- b) Roles y responsabilidades de los participantes en la gestión de continuidad del negocio, incluyendo a la Unidad de Informática;
- c) El análisis de impacto del negocio (BIA), en el cual se tome en cuenta lo siguiente:
 - i. todos los productos y servicios que proporciona el Fondo;
 - ii. Identificación de los sistemas y servicios de TI críticos y los procesos relacionados a ellos;
 - iii. La identificación, cuantificación y calificación de los impactos de incidentes de interrupción en términos financieros, reputacionales, operativos y legales;
 - iv. El tiempo máximo del período tolerable de interrupción (MTPD), el tiempo objetivo de recuperación (RTO), punto objetivo de recuperación (RPO), objetivo mínimo de continuidad de negocio (MBCO);
 - v. Señalar las dependencias y recursos de apoyo para estas actividades.

Además, los resultados del BIA servirán de base para definir aspectos relacionados a redundancia de equipos y suministro de energía eléctrica, y el centro de datos alterno.

- d) Análisis de amenazas a la continuidad de negocio;
- e) Pruebas a los planes de continuidad del negocio;
- f) Integración de la gestión de la continuidad del negocio dentro de la cultura organizacional a través de la capacitación, divulgación y concientización del personal, al menos una vez al año.

- 4.2. FOPROLYD no cuenta con un Plan de Recuperación de Desastres, en el cual se defina el conjunto de procedimientos y planes de acción, la definición de los roles y responsabilidades de los encargados de su ejecución, que permitan mantener la continuidad de la plataforma tecnológica de la entidad, en caso de la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente; así como se incluya la ejecución de pruebas a dicho plan de manera periódica, y cuyos resultados sean documentados por medio de un informe formalizado que contenga los resultados obtenidos, las recomendaciones y los acuerdos para implementar mejoras de manera oportuna, y que sea del conocimiento de la Junta Directiva o de quienes hagan sus funciones.
- 4.3. FOPROLYD no cuenta con una política de gestión de proyectos, que les proporcione los lineamientos generales para gestionar los mismos, tanto a nivel de Hardware como de Software que surjan en el Fondo, mediante la cual se definan parámetros específicos para determinar las prioridades de los requerimientos de los usuarios, los niveles de aprobación respectivos, que permita que los proyectos propuestos no puedan comenzar sin la debida autorización.
- 4.4. Dentro del Manual de Políticas, Normas y Procedimientos de la Unidad de Informática de FOPROLYD, no se han incluido aspectos relacionados a la definición de estándares para el proceso de desarrollo de software con el objetivo de aplicar las mejores prácticas de la ingeniería de software para garantizar la calidad y seguridad en cada uno de los aplicativos y sistemas de información desarrollados.
- 4.5. En FOPROLYD no existen lineamientos sobre mecanismos de comunicación y escalamiento de aspectos críticos relacionados con Tecnología, que deban ser informado hacia Gerencia General y la Junta Directiva, así como la falta de definición de parámetros para comunicar dichos aspectos, ya que todo depende de los informes que la Unidad de Informática presenta a la Gerencia General.

- 4.6. FOPROLYD no cuenta con una adecuada separación entre los ambientes de desarrollo y producción, ya que los proyectos de desarrollo de sistemas dentro de la Unidad de Informática se construyen en un ambiente de desarrollo local a través de los técnicos responsables del sistema, sin embargo, trabajan sobre la misma base de datos puesta en producción, lo que expone a riesgos que podrían afectar la seguridad de la información ahí contenida.
- 4.7. Se determinó que los Técnicos de Informática de FOPROLYD, tienen acceso a los sistemas y bases de datos en ambiente de producción, sin que existan controles suficientes para monitorear dichos accesos, de tal manera que se garanticen la integridad y confidencialidad de la información.
- 4.8. Se determinó que en FOPROLYD la información sensible como las contraseñas de los usuarios, no es almacenada en las tablas con las medidas de seguridad necesarias para mantener la confidencialidad de éstas, por lo que todo el que tenga acceso a dichas tablas, puede tener acceso a la información de los usuarios y conocer las contraseñas.
- 4.9. En el Manual de Organización y Descripción de Puestos de Trabajo de FOPROLYD, no existe una clara separación de las funciones específicas que realizan los técnicos de informática, ya que no se detallan las funciones del personal que realiza mantenimiento de sistemas y del personal de soporte de operaciones de TI (soporte para redes, centro de datos, sistemas operativos, etc.). así como tampoco cuentan con mecanismos y controles que permitan un adecuado monitoreo de los accesos a los sistemas y bases de datos por personal que por sus funciones, no necesitan tener acceso a los mismos. Además, tampoco existe una adecuada segregación de funciones, ya que el mismo técnico que desarrolla o modifica los sistemas, es el mismo que realiza las pruebas y administra posteriormente todo lo relacionado a los mismos: creación y modificación de usuarios, administración de la base de datos del sistema, etc.. así como tampoco cuentan con controles que aseguren que los riesgos identificados se manejan de forma adecuada.

4.10. En la revisión que realizó el Instituto de Previsión Social de la Fuerza Armada (IPSFA) a los sistemas informáticos del Fondo en el año 2015, se determinaron 7 observaciones de las cuales a la fecha únicamente en 3 han realizado acciones que solventan de forma parcial dichas observaciones; y con respecto a las 10 observaciones que quedaron en proceso en la evaluación del 2017, únicamente en una de ellas se realizaron acciones para solventarla parcialmente. Las observaciones no atendidas y que se clasifican con criticidad alta, se mencionan a continuación:

- a) Deficiencias en controles de seguridad física en área de servidores; UPS en área de Servidores sin redundancia;
- b) Servidores y Switches sin una adecuada protección y ubicación;
- c) Cableado enredado, suelto y sin identificación;
- d) Servidores con sistemas operativos sin soporte técnico del fabricante;
- e) No se cuenta con un lugar alternativo para respaldo y recuperación de las operaciones de la institución;
- f) Perfiles sin reflejar las funciones específicas ejercidas por el personal de la Unidad de Informática;
- g) Plan de Contingencia sin acciones concretas que garanticen la continuidad de las operaciones y procesos críticos;
- h) Usuario genérico compartido por el personal de la Unidad de Informática para realizar funciones de Administrador de red.

5. SEGUIMIENTO A RECOMENDACIONES CONTENIDAS EN LOS INFORMES DE AUDITORIAS ANTERIORES REALIZADAS POR AUDITORIA INTERNA, CORTE DE CUENTAS Y FIRMAS PRIVADAS.

5.1. AUDITORIA INTERNA.

A efecto de dar seguimiento a las recomendaciones contenidas en el informe de auditoría y al cumplimiento al Art. 118, se le dieron seguimiento a las siguientes recomendaciones:

SEGUIMIENTO A RECOMENDACIONES INFORMES 2015 Y 2017

Observación 2015	Acciones Ejecutadas - comentario FOPROLYD 2020	Seguimiento SSF
<p>1. Deficiencias en controles de seguridad física, en área de servidores.</p> <p>En el área de servidores de la Unidad de Informática, donde se concentra la mayoría de los equipos tecnológicos (servidores, "switch", dispositivo de almacenamiento masivo de datos, firewall, etc.) que manejan los programas e información sensible de FOPROLYD; identificamos deficiencias en cuanto a la seguridad física, las cuales se detallan a continuación:</p> <p>a) El aire acondicionado no cuenta con la tecnología (sistemas de alarmas y control de humedad) que permita comunicar al personal fallas y/o variaciones importantes como desconexión, cambios de temperatura, humedad, etc., que afecten los equipos tecnológicos.</p> <p>b) No existe una bitácora que permita controlar la hora de entrada y salida del personal interno o externo y el motivo por el cual ingresó al área de servidores.</p>	<p>a) El aire acondicionado sigue en las mismas condiciones, se le ha solicitado el cambio de los aires en múltiples ocasiones a la administración superior sin realizar ningún cambio hasta la fecha.</p> <p>b) Ya contamos con una bitácora que permite controlar la hora de entrada del personal interno no así la hora de salida ni el motivo por el cual entró al área de servidores.</p> <p>c) Ya se cuenta con seguridad de acceso.</p> <p>d) Ya no se realizan labores cotidianas en el área de servidores.</p> <p>Se anexan Fotos</p>	<p>a) De acuerdo con fotografía proporcionada por el Fondo, se observa que el aire acondicionado del Centro de Datos mantiene las observaciones determinadas en la visita 2015.</p> <p>b) El log que se genera por medio del sistema que controla las puertas con accesos biométricos, no constituye una bitácora de acceso, ya que no le permite a la entidad controlar quien(es) ingresan al centro de datos, el motivo del ingreso, el tiempo que pasa dentro del centro de datos, etc.</p> <p>c) Según lo manifestado por el personal de la entidad, la seguridad de acceso corresponde a un control biométrico por huella dactilar para poder ingresar al centro de datos. Sin embargo, manifiestan que debido a que en el centro de datos también se encuentra instalada la central telefónica, aparte del personal de la Unidad de Informática, tienen acceso al centro de datos.</p> <p>d) personas de mantenimiento de servicios generales. Al respecto,</p>

<p>c) El área de servidores no cuenta con la suficiente seguridad de acceso.</p> <p>d) La seguridad del área de servidores tiene un alto riesgo ya que personal técnico de la Unidad de Informática realiza labores cotidianas en el área de Servidores, para lo cual cuenta con un escritorio, archivos, mesa de trabajo, entre otros.</p>		<p>se considera que se deben revisar los permisos de acceso asignados, ya que aún hay muchas personas que pueden ingresar al centro de datos.</p>
<p>2. Deficiencias en el control de inventario del equipo informático. En la verificación física efectuado al inventario del equipo informático de la Unidad de Informática, se determinaron las siguientes inconsistencias:</p> <p>a) Equipo que físicamente no cuenta con su respectiva codificación: 2 racks en el área de servidores, no se encuentran en inventario de la Unidad de Informática.</p> <p>b) Equipos que no se encuentran inventariados: Dos discos duros para servidores.</p> <p>c) Equipos que se encuentran en el reporte de inventario y que físicamente no se encontraron: Dos discos duros.</p> <p>d) Sin descargo UPS dañado, con código EI-11-211 UPS- SMART, se encuentra en el área de servidores.</p>	<p>a) Se codificó todo el equipo informático.</p> <p>b) Se codificaron los dos discos duros para servidores, así como todo el equipo que se ha adquirido hasta la fecha.</p> <p>c) Se encontraron los dos discos duros y se descargaron por obsolescencia.</p> <p>d) Se realizó el descargo de UPS dañado con código EI-11-211.</p> <p>e) Se descargaron las dos antenas tipo plato.</p> <p>f) Se procedió a realizar la descarga de dichos equipos.</p> <p>Se anexa documentación de descargo</p>	<p>Aún persisten deficiencias en el control de inventarios de equipo, ya que en el documento presentado que corresponde al listado de equipos descargados de la Unidad de informática, en el cual se observaron siguiente:</p> <p>a) No se evidencia la codificación de los 2 racks en el área de servidores, ni el ingreso al inventario de la unidad de informática.</p> <p>b) No se evidencia el ingreso al inventario de dos discos duros para servidores.</p> <p>c) Dos discos duros identificados con el código EI-27-4 y EI-27-5 ya fueron descargados del inventario de la Unidad de Informática.</p> <p>d) No se evidencia el descargo del UPS con código EI-11-211 UPS SMART.</p>

<p>e) Equipo informático subutilizado: Dos antenas tipo plato, sin utilizarse, en área de servidores, valor actual en libros \$173.05, valor compra \$1.845.00</p> <p>f) Equipo asignado según reporte de Activo Fijo al Técnico Programador físicamente fue encontrado en el Área de Servidores.</p>		<p>e) Dos antenas tipo plato ya fueron descargadas del inventario de la Unidad de Informática.</p> <p>f) No se evidencia el descargo del equipo asignado según reporte de Activo Fijo al Técnico Programador que fue físicamente encontrado en el Área de Servidores.</p>
<p>3. UPS en área de Servidores sin Redundancia: Todos los equipos informáticos en el área de servidores se encuentran conectados a un UPS, éste por sí solo no proporciona redundancia, ante un corte de energía prolongado; no se podría proceder al correcto apagado de los servidores, con la posible pérdida de los datos y daño a los equipos.</p>	<p>Se mantiene en el área de servidores sin redundancia.</p>	<p>La observación no ha sido subsanada</p>
<p>4. Servidores y switches no cuentan con una adecuada protección y ubicación. Los servidores y switches no cuentan con una adecuada protección y ubicación que los proteja de cualquier tipo de manipulación física o de accidentes; como derrames de café. Polvo. etc.; los servidores están ubicados sobre mesas sin ninguna protección, esto puede ocasionar que los equipos se dañen y se genere interrupción de los diferentes servicios prestados por la Unidad de Informática; así como</p>	<p>Ya se procedió a montar los switch y servidores en sus respectivos racks para su adecuada protección.</p>	<p>Los switch y servidores ya fueron instalados en sus respectivos racks. Sin embargo, aún se observa equipo sin la debida protección, además que han colocado recipientes plásticos sobre los racks lo que evidencia filtraciones de agua en el cielo falso y/o problemas de goteo de los aires acondicionados poniendo en peligro el equipo ahí resguardado.</p>

<p>la posible pérdida de información de FOPROLYD.</p>		
<p>5. Cableado enredado, suelto y sin identificación. El cableado utilizado para el ambiente de borde y servidores se encuentra de forma dispersa y enredada; además no cuentan con ningún tipo de identificación, situación que impediría una atención oportuna a los usuarios al no poderlos identificar y además no permite una adecuada circulación del aire, lo que limita la efectividad de enfriamiento de los equipos</p>	<p>Se mantiene la observación.</p>	<p>La observación se mantiene</p>
<p>6. Servidores con sistemas operativos Windows server 2000 y 2003, sin soporte técnico del fabricante. Un servidor con el sistema operativo 2000, no tiene asistencia de soporte ni actualizaciones de seguridad, desde el 13 de julio del 2010. Así mismo, se encuentran dos servidores con sistema operativo instalado, Windows Server 2003, cuyo soporte técnico de Microsoft finaliza el 14 de julio de 2015. A partir de dicha fecha cuando ya no se proporcionarán actualizaciones ni revisiones se producirá una pérdida de cumplimiento de cualquier centro de datos que ejecute este Sistema Operativo, existiendo el riesgo de posible penetración de intrusos, por falta de actualizaciones o parches. De acuerdo con Windows, los clientes que tengan instalada una versión no admitida de</p>	<p>Hasta la fecha se mantiene los servidores con sistemas operativos Windows server 2000 y 2003. Se acaban de adquirir 4 Licencias de Windows Server 2019 las cuales se utilizarán para cambiar dichos servidores con sistemas operativos Windows Server 2000 y 2003 sin soporte Técnico del fabricante.</p>	<p>La observación se mantiene debido a que aún no han sido cambiados los servidores observados por las licencias de Windows Server 2019 adquiridas.</p>

<p>Windows o Service Pack, no serán elegibles para ninguna opción de soporte técnico.</p>		
<p>7. No se cuenta con un lugar alternativo para respaldo y recuperación de las operaciones de la institución, ni con un plan de contingencia. FOPROLYD carece de un sitio alternativo para respaldo y Recuperación, así como de un plan de contingencia de la información, que garantice la continuidad de las operaciones y procesos críticos, ante un eventual desastre, ya sea natural (terremoto, huracán, etc.) o provocado por el hombre (vandalismo). Ante un evento adverso de la naturaleza o provocado por el hombre, la falta de planeamiento y definición de acciones concretas para la creación y aplicación de estrategias de resguardo de la información, sumado a la inexistencia de planes de recuperación y de continuidad de las operaciones, podrían provocar interrupciones prolongadas en procesos críticos de la institución, con un impacto alto en actividades claves, afectando a sus diferentes usuarios, tanto internos como externos, pudiendo llegar a una negación de servicios; con el deterioro de imagen respectivo.</p>	<p>Seguimos sin contar con un lugar alternativo para respaldo y recuperación de las operaciones de la institución ni con un plan de contingencia.</p>	<p>La observación se mantiene</p>

Observación 2017	Acciones Ejecutadas Comentario FOPROLYD 2020	Comentario SSF
<p>1. Debilidades en los expedientes de personal de la Unidad de Informática.</p> <p>a) Técnicos Informáticos, Oscar Guillermo Flores Calderón con título obtenido como Técnico en Ingeniería en Computación y Álvaro Ramón Henríquez Alas c/p Juan José Henríquez con diploma Técnico en Computación Programador Analista, no han cumplido con requisito de grado, que requiere el perfil del puesto para los Técnicos Informáticos; de acuerdo al Manual de Descripción de Puestos y Funciones de la Unidad de Informática, deberán ser egresados o graduados en Ingeniería o Licenciatura en Ciencias de la Computación.</p> <p>b) En los expedientes de los empleados José Ulises Montoya Polanco, José Ricardo Oliva Aguirre y Álvaro Ramón Henríquez Alas, no identificamos referencias personales.</p> <p>c) Las copias de títulos o certificados de grado académico, obtenidos por personal de la Unidad de Informática, no se encuentran debidamente certificados por Notario, ni existe evidencia de haber sido confrontados con su original.</p>	<p>a) El técnico Oscar Guillermo Flores Calderón decidió continuar sus estudios los cuales está cursando actualmente según Memorándum, para cumplir con el requisito de grado que se requiere; se desconoce la situación del Técnico Álvaro Ramón Henríquez.</p> <p>b) Memorándum Ref. RRHH207/2018 el cual se anexa.</p> <p>c) En los expedientes de los empleados José Ricardo Oliva Aguirre y José Ulises Montoya Polanco ya se les anexo las referencias personales correspondientes.</p> <p>d) Las copias de títulos o certificados de grado académico, obtenidos por personal de la Unidad de Informática ya se encuentran debidamente certificados por Notario.</p>	<p>Con respecto al requisito de grado académico establecido en el Manual de Descripción de Puestos y Funciones de la Unidad de Informática debido al tiempo de experiencia en el cargo que tienen los técnicos informáticos mencionados en la observación, se recomienda como medida alternativa, que FOPROLYD defina parámetros de evaluación del desempeño del trabajo realizado por dichos empleados, a fin de determinar la idoneidad al cargo, mientras no cumplan con lo establecido en el Manual antes mencionado.</p>

<p>2. Perfil de Técnico Informático no refleja las funciones específicas ejercidas por personal de la Unidad de Informática.</p> <p>En verificación de las funciones del personal de la Unidad de Informática, observamos que no refleja las funciones específicas ya que todas las funciones de los analistas programadores, soporte técnico, base de datos, administrador de red, administrador de antivirus, están incluidas en el Perfil del Técnico Informático.</p>	<p>Se mantiene dicha Observación actualmente ya que no se ha realizado ninguna modificación al respecto.</p>	<p>Se mantiene la observación.</p>
<p>3. Falta de Manuales Técnicos que soporten los Sistemas Informáticos desarrollados.</p> <p>En entrevista sostenida con el Ing. José Ulises Montoya Polanco, el día 3 de octubre de 2017, donde se le consultó sobre la existencia de los Manuales Técnicos, de los Sistemas desarrollados por personal de FOPROLYO, se nos manifestó que no cuentan con manuales técnicos de los sistemas informáticos desarrollados.</p>	<p>No se han realizado cambios al respecto.</p>	<p>Se mantiene la observación.</p>
<p>4. No existen estándares de desarrollo para los sistemas informáticos.</p> <p>En entrevista sostenida con el Ing. José Ulises Montoya Polanco. el día 3 de octubre de 2017, donde se le consultó sobre la existencia de estándares de programación para el desarrollo de sistemas, nos manifestó que no cuentan con estándares de programación para el desarrollo de los Sistemas Informáticos</p>	<p>No se han realizado cambios al respecto.</p>	<p>Se mantiene la observación.</p>
<p>5. Plan de Contingencia de la Unidad de Informática carece</p>	<p>No se han realizado cambios al respecto.</p>	<p>La observación se mantiene.</p>

de acciones concretas, que garantice la continuidad de las operaciones y procesos críticos de FOPROLYD.

En verificación del Plan de Contingencia de la Unidad de Informática, contenido en el Manual de Políticas, Normas y Procedimientos, se constató que ante un evento adverso de la naturaleza o provocado por el hombre, la falta de planeamiento y definición de acciones concretas para la creación y aplicación de estrategias de resguardo de la información, sumado a la inexistencia de planes de recuperación y de continuidad de las operaciones, podrían provocar interrupciones prolongadas en procesos críticos de la institución, con un impacto alto en actividades claves, afectando a sus diferentes usuarios, tanto internos como externos, pudiendo llegar a una negación de servicios; con el deterioro de imagen respectiva.

Esta observación fue realizada en Informe de Auditoría al 31 de marzo de 2015, Auditoría Informática a la Seguridad de los Sistemas de TI, de FOPROLYD, hasta el momento se encuentra en proceso, ya que no se han definido en dicho plan, el conjunto de pasos o procedimientos necesarios para recuperar y estabilizar las operaciones informáticas en la Entidad, en caso de producirse una eventualidad que afecte la operación normal de los sistemas de información. Dicho plan debe contener las medidas técnicas, humanas y organizativas necesarias para garantizar la

<p>continuidad del negocio y las operaciones de la institución, considerando entre las acciones a realizar la coordinación de áreas competentes en la materia. como son Cuerpo de Bomberos, suplidores de servicios (energía eléctrica, comunicaciones), Cruz Roja, entre otros, y personal interno de la institución que esté involucrado en los diferentes servicios que garanticen la continuidad de las operaciones</p>		
<p>6. Matriz de Riesgo Tecnológica con debilidades. En la verificación de la Matriz de Riesgos Tecnológicos, del período 2017 - 2018, comprobamos que la descripción de las acciones o actividades a realizar para mitigar los riesgos, están descritas de forma general lo que limita el seguimiento, no se especifica el responsable, fecha de ejecución de la actividad, ni el monto de la inversión o gasto para mitigar el riesgo.</p>	<p>No se han realizado cambios en dicha observación.</p>	<p>Se mantiene la observación.</p>
<p>7. Requerimientos de la Unidad de Informática son controlados por medio de correo electrónico. Identificamos que los requerimientos referentes a soporte y mantenimiento de software y hardware tanto de la red como de los sistemas; son administrados por medio de correos electrónicos; lo que comprueba que la Unidad de Informática no cuenta con un control administrativo que identifique los distintos requerimientos que categorice, Diagnostique, registre errores y la frecuencia de éstos. evalúe problemas graves, que cuente</p>	<p>No se han realizado cambios en dicha observación.</p>	<p>Se mantiene la observación.</p>

<p>con fecha de solicitud y atención del mismo; también no es posible generar reportes con el detalle de requerimientos (incidencias) resueltos y pendientes de un período determinado ni es posible generar informes que reflejen el trabajo realizado por la Unidad de Informática y la satisfacción del cliente interno.</p>		
<p>8. La Unidad de Informática no cuenta con procedimiento para el control de cambios en los sistemas.</p> <p>Como resultado del cuestionario de control interno enviado al Jefe de la Unidad de Informática. Comprobamos que no existe procedimiento para el control de cambios (versiones del Sistema), ni control de versionamiento de modificaciones realizadas a los sistemas desarrollados en la Unidad de Informática de FOPROLYD.</p>	<p>No se han realizado cambios en dicha observación.</p>	<p>Se mantiene la observación.</p>
<p>9. Usuario genérico es compartido por personal de la Unidad de Informática, para realizar funciones de Administrador de Red.</p> <p>En verificación del Active Directory (Servicios de Directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración) en conjunto con el Administrador de Red, Técnico Informático Álvaro Ramón Henríquez Alas, identificamos que existe un solo usuario administrador con todos los privilegios, que permiten navegar en toda la red, ingresar, modificar, eliminar usuarios del dominio (red institucional), asignar</p>	<p>No se han realizado cambios en dicha observación.</p>	<p>Se mantiene la observación.</p>

<p>roles y privilegios a usuarios de la red. Este usuario administrador, es compartido (un único usuario) por todo el personal de la Unidad de Informática, para dar soporte a usuarios de la red de FOPROLYD, por lo que no es posible identificar o individualizar al personal que realizó la acción ni establecer o determinar responsabilidades en caso de fraudes o incidencias graves.</p>		
<p>10. No existe una separación de funciones en los ambientes de desarrollo y producción. En entrevista in situ con dos técnicos informáticos, con funciones de analistas programadores, responsables de los sistemas, Atención a Beneficiarios/Expediente electrónico-SIABES, Migración de Sistemas Administrativos/Financieros y Administración de Personal; identificamos, que éstos cuentan con accesos a la base de datos de producción, siendo los responsables de crear usuarios y asignar roles (permisos) de los sistemas.</p>	<p>No se han realizado cambios en dicha observación.</p>	<p>Se mantiene la observación.</p>

5.2. AUDITORIA EXTERNA:

A la fecha de la emisión del presente informe la Unidad de Auditoría Interna no tiene conocimiento que existan recomendaciones pendientes de cumplir que hayan sido emitidas por firmas privadas de auditoría y que estén relacionadas con los Sistemas Informáticos de FOPROLYD.

5.3. CORTE DE CUENTAS DE LA REPÚBLICA.

A la fecha de la emisión del presente informe la Unidad de Auditoría Interna no tiene conocimiento que existan recomendaciones pendientes de cumplir que hayan sido emitidas por la Corte de Cuentas de la República y que estén relacionadas con los Sistemas Informáticos de FOPROLYD.

6 RECOMENDACIONES DE AUDITORIA.

De acuerdo a los resultados de auditoría comunicados por la Superintendencia del Sistema Financiero, es necesario:

- 6.1. Un mayor involucramiento de la Alta Administración para velar que se elabore un plan de acción que contenga como mínimo el detalle de las actividades a realizar para solucionar todos los aspectos observados en el numeral 4 del presente informe; incluyendo fechas y responsables de cada actividad, lo cual deberá ser comunicado a Gerencia General y Junta Directiva para que realicen el seguimiento respectivo.
- 6.2. Generar instrucciones a las áreas involucradas de dar cumplimiento al detalle las observaciones que se encuentran pendientes de auditorías anteriores y que se encuentran detalladas en el numeral 5 del presente informe.

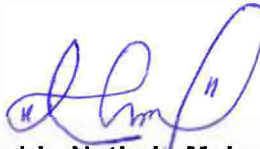
7 CONCLUSIÓN.

De acuerdo a los resultados obtenidos, se concluye que los sistemas informáticos y demás recursos tecnológicos de FOPROLYD actualmente no cuentan con los controles internos, administración de riesgos, planificación y organización de recursos, entrega y soporte de servicios, monitoreo y evaluación de los recursos tecnológicos que permitan a FOPROLYD contar con seguridad razonable de los Sistemas Informáticos y demás recursos tecnológicos.

8 PÁRRAFO ACLARATORIO.

El presente informe contiene los resultados obtenidos de la auditoría a los Sistemas Informáticos de FOPROLYD al 31 de diciembre de 2020, ha sido elaborado para informar a la Honorable Junta Directiva y funcionarios relacionados, el examen comprendió las principales actividades relacionadas al control interno informático que se ejecutan sobre los sistemas informáticos de FOPROLYD con un alcance específico, por lo que no se emite opinión sobre la razonabilidad de las cifras presentadas en los estados financieros, o detallar situaciones específicas que por las características que presentan constituyan riesgos potenciales.

DIOS UNIÓN LIBERTAD



Licenciada Iris Nathaly Melgar Mercado
Supervisora y Jefa Interina de la Unidad de Auditoría Interna