Bogotá, 10 de enero de 2014

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO -SARO-
Octubre-Diciembre 2013

CAPROVIMPO por ser un entidad de carácter financiero, organizada como establecimiento de crédito, de naturaleza especial, vigilada por la Superintendencia Financiera de Colombia (SFC), en desarrollo de su objeto social está expuesta al Riesgo Operativo, por lo que en cumplimiento de las directrices dadas por la SFC adoptó un Sistema de Administración de Riesgo Operativo -SARO-, el cual debe ser desarrollado, establecido, implementado y actualizado.

En cumplimiento de las instrucciones de actualización aprobada por la Junta Directiva en enero de 2013, se realizaron ajustes en la metodología aplicada en el SARO especificando: estrategias, técnicas e instrumentos, con el propósito de alcanzar los objetivos de cada una de las etapas de la administración del riesgo, logrando de esta manera dar cumplimiento a los requisitos establecidos en el Capítulo XXIII de la Circular Básica Contable y Financiera de la SFC.

De tal modo que para el cuarto trimestre del 2013, se tiene un total de 74 Riesgos Operativos identificados para la Entidad, los cuales se listan a continuación:

RO	Riesgo Operacional
1	Errores o inconsistencias en la información de la cuenta individual y la hoja de vida del afiliado
2	Fallas en la liquidación de intereses de la cuenta del afiliado
3	Errores y/o demoras en la devolución de aportes/cesantías
4	Apropiación indebida de recursos
5	Fallas en los sistemas de información
6	Deficiencias en el trámite de embargos y desembargos
7	Errores en las novedades a reportar a las unidades ejecutoras
8	Errores en la elaboración de la planilla de pago del subsidio
9	Demoras en el trámite de solicitud del subsidio
10	Incumplimiento de la normatividad
11	Incumplimiento y/o inconsistencias en la entrega de información a Entes de Control

12	Inconsistencias en reportes entregados a la Alta Gerencia
13	Fallas en la ejecución de la orden de negociación
14	Errores o inconsistencias en la valoración del portafolio de inversiones
15	Fallas en el registro de inversiones
16	Atención, orientación y/o asesoría inadecuada
17	Fallas en la gestión del trámite
18	Inconsistencias en la base de datos de afiliados
19	Extravío y/o deterioro de la documentación
20	Incumplimiento del Outsourcing
21	Falsificación documental y/o suplantación de identidad
22	Inconsistencias y/o inoportunidad en la respuesta a la solicitud realizada por el consumidor financiero
23	Problemas con los proyectos inmobiliarios promocionados
24	Fallas en la gestión de solución de vivienda para el Fondo de Solidaridad
25	Fallas o debilidades en la administración del encargo fiduciario del Fondo de Solidaridad
26	Inconsistencias en el contenido de las comunicaciones externas
27	Apropiación ilícita de recursos del Fondo de Solidaridad
28	Negligencia en el reporte y documentación de los riesgos
29	Fallas en la administración del Plan de Continuidad del Negocio -PCN-
30	Concentración de funciones
31	Pérdida de talento
32	Incumplimiento en la generación y envío de informes a autoridades administrativas y de gobierno
33	Deficiencias en la elaboración y validación de la planificación de la gestión estratégica de la Entidad
34	Deficiencias en el seguimiento a los planes de gestión y mejoramiento de la Entidad
35	Deficiencia en la calidad y oportunidad en la entrega de la información requerida
36	Debilidades en las competencias requeridas por el equipo auditor
37	Fallas y/o demoras en la generación de la certificación de cumplimiento para pago a contratistas
38	Contratación de un bien o servicio que no cumpla con los términos de referencia
39	Fallas o demoras en la elaboración del Plan de Contratación
40	Demoras o fallas en la representación judicial y extrajudicial de la Entidad
41	Errores en la emisión de conceptos jurídicos
42	Fallas en la actualización de la normatividad aplicable a CAPROVIMPO en los sistemas de información
43	Error o demoras en el ingreso y distribución de la documentación y comunicaciones
44	Error o demoras en la salida de documentación y comunicaciones de la Entidad
45	Completitud y confiabilidad del archivo digital
46	Fallas en la vinculación del personal
47	Errores en la liquidación de nómina

48	Fallas en la capacitación del personal
49	Fallas en la elaboración y ejecución del Plan de Bienestar Integral
50	Fallas en la desvinculación laboral
51	Fallas y/o demoras en la distribución de los elementos requeridos por los procesos
52	Fallas en la administración del inventario
53	Fallas en la administración de la caja menor
54	Fallas en la administración de inmuebles
55	Errores o demoras en la elaboración y presentación del proyecto Manual de Presupuesto
56	Afectación errónea de los rubros presupuestales
57	Errores en la elaboración de comprobantes de ingresos
58	Demoras en el trámite de las órdenes de pago
59	Errores en la ejecución de los pagos
60	Fallas y/o extemporaneidad en la liquidación, presentación y pago de obligaciones tributarias
61	Incumplimiento Acuerdo de Niveles de Servicio y/o Contratos de mantenimiento/soporte
62	Interrupción parcial o total de los servicios ofrecidos por TI
63	Fallas en los planes de contingencias de TI
64	Ausencia total y/o parcial de contratos de soporte y mantenimiento de los servicios de TI
65	Utilización indebida de información confidencial
66	Falta de personal
67	Procedimientos no documentados y/o se encuentran desactualizados
68	Insuficiencia, obsolescencia y/o subutilización de los activos tecnológicos
69	Fallas de conectividad
70	Interrupción en el servicio del centro de computo
71	Fallas en la disponibilidad de los sistemas de información
72	Fallas en el respaldo y recuperación de la información
73	Fallas en el seguimiento y control a contratos de tercerización
74	Vulneración de la integridad, disponibilidad y confidencialidad de la información de la Entidad

Los Riesgos Operativos identificados para CAPROVIMPO tienen la siguiente distribución de criticidad, de acuerdo a su calificación residual:

		Riesgo Residual Actual	
Riesgos Operativos identificados	74	Riesgo Operativo Extremo	0
		Riesgos Operativo Alto	6
		Riesgo Operativo Moderado	41
		Riesgo Operativo Menor	26
		Riesgo Operativo Bajo	1

Teniendo en cuenta la efectividad de los controles sobre los Riesgos Operativos y en concordancia con la dinámica de CAPROVIMPO, el perfil de riesgo residual actual se ubica en el nivel moderado-menor con una calificación de 8.34.

REGISTRO DE EVENTOS DE RIESGO OPERATIVO -RERO-

Durante el periodo comprendido entre octubre y diciembre del 2013, se ha realizado el registro y análisis de los eventos de Riesgo Operativo reportados por los líderes de los procesos y de aquellos identificados por la Oficina Asesora de Gestión del Riesgo, en total se presentaron 104 REROS, los cuales de acuerdo a lo establecido por la SFC están clasificados como sigue:

Clasificación	Eventos con pérdida	Eventos sin pérdida	Total Eventos
Ejecución y administración de procesos	0	78	78
Fallas tecnológicas	0	10	10
Fraude externo	0	12	12
Eventos Externos	0	4	4
TOTAL	**0**	**104**	**104**

Vale la pena destacar que se presentaron 12 eventos potenciales de fraude externo los cuales ascienden a la suma de $ 151.424.702, pero gracias a los controles establecidos por la entidad y a las acciones adelantadas por el Grupo de Seguridad Documental, los mencionados intentos no se materializaron evitando pérdidas a la entidad.

De los eventos materializados, ninguno constituyó pérdidas económicas para la Entidad.

PRODUCTO NO CONFORME

Como insumo para la identificación de riesgos, se lleva a cabo el control estadístico del Producto No Conforme –PNC-. El grupo de Sistema de Atención al Consumidor Financiero, el Grupo de Cuentas Individuales, el Grupo de Cesantías, Servicio al Afiliado y sus Puntos de Atención reportaron 73 registros de PNC durante el cuarto trimestre del 2013, distribuidos como sigue:

Proceso	Producto No Conforme
Sistema de Atención al Consumidor Financiero -SAC-	5
Grupo de Cuentas Individuales	23
Grupo de Cesantías	12
Servicio al Afiliado y Puntos de Atención	33
Total	**73**

Los registros del reporte de Producto No Conforme fueron analizados por la Oficina Asesora de Gestión del Riesgo concluyendo que constituyen eventos de Riesgo

Operativo; sin embargo, no hay elementos que generen alertas tempranas o evidencien la materialización de nuevos Riesgos Operativos.

PLAN DE CONTINUIDAD DEL NEGOCIO

A nivel de Organización se mantienen los esquemas de seguridad garantizando la protección de la información.

Se suscribió el contrato No. 114 del 13 de septiembre de 2013, con TELMEX S.A. DE COLOMBIA del Plan de Continuidad de Negocio, realizándose las siguientes actividades:

1. Ejecución de la conectividad entre el DCP (Triara) y el DCA (Ortezal), con ejecución de pruebas satisfactorias entre los dos puntos.
2. Ejecución de la Instalación, configuración de Hardware y software de la infraestructura para el ambiente de replicación:

    a. 2 Servidores físicos en cluster, Sistema operativo Windows Server 2012 y herramienta de replicación Hyperview de Microsoft.
    b. Almacenamiento con capacidad para 15 GB.

3. Replica y validación del ambiente de los siguientes Sistemas de Información y sus bases de datos, definidos en el PCN:
    i. FENIX
    ii. SAC
    iii. FOLIUM
    iv. VIGIA
    v. MONITOREO Y CONTROL
    vi. GA2
    vii. SEVEN
    viii. DIALOGO
    ix. ORION
    x. EXCHANGE
    xi. BISTALK
    xii. PORTAL WEB
    xiii. INTRANET

4. De las pruebas de validación de réplica de los S.I. se evalúa que hay una sincronización de un margen de 5 minutos, lo cual es altamente significativo para el tiempo RTO y RPO fijados en 3 y 1 hora respectivamente.

5. Se realizó levantamiento de información para el desarrollo de la documentación de la FASE 1 en versión 001 del PCN, para dar cumplimiento a lo estipulado en la norma ISO 22301:2012 y las fijadas por la SFC.

CAPACITACIONES

La Oficina Asesora de Gestión del Riesgo en su función de diseñar, programar y coordinar planes de capacitación sobre el SARO dirigidos a todas las áreas y funcionarios, durante el cuarto trimestre de 2013, brindó inducción a 116 funcionarios que ingresaron a la Entidad, tal como se muestra a continuación:

Inducción	Funcionarios Capacitados	Calificación Promedio
Octubre	3	96.6
Noviembre	84	95.75
Diciembre	29	89.6

SEGURIDAD DE LA INFORMACIÓN

A continuación se exponen todos los ítems a los cuales el Grupo de Seguridad de la Información realiza seguimiento y controles requeridos para cada tema.

Informe trimestral Monitoreo y Seguimiento control de fuga de información.

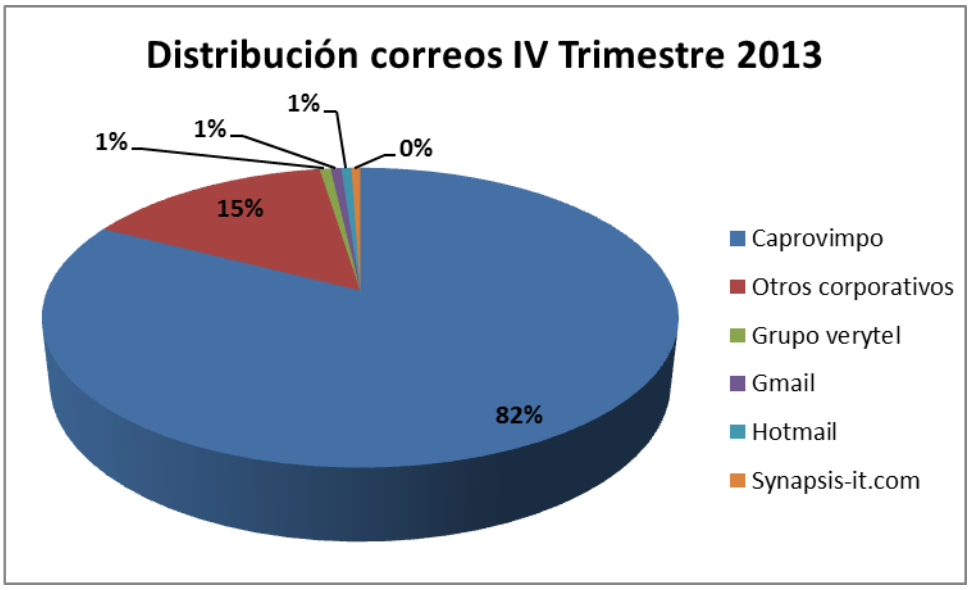
El grupo de Seguridad de la Información realiza monitoreo permanente al uso adecuado de las herramientas de correo y al manejo de la navegación, el cual es exclusivo de la entidad con fines laborales y de consulta. Previniendo posibles eventos de fuga de información, eventos de denegación de servicios, así como monitoreando el tráfico autorizado en servicios como FTP, Telnet, SNMP, SSL, SMTP, HTTP, "correo", entre otros.

Para el caso del correo electrónico, durante el 4 trimestre de 2013, se evidencio un total de 943.654 correos distribuidos de la siguiente manera:

NOMBRE CUENTA	No. Correos	Participación
Caprovimpo	779,443	82.60%
Otros corporativos	141,020	14.94%
Grupo Verytel	6,290	0.67%
Gmail	6,087	0.65%
Hotmail	5,729	0.61%
Synapsis-it.com	5,085	0.54%
Total	943,654	100.00%

Se detectó violación de las políticas de seguridad en un 0.3 % del tránsito de correos; de los cuales 0.2% fue justificada por cuestiones del servicio y un 0.1% que no representa ninguna gravedad o posibles fugas de información pero que cumpliendo

con nuestros procedimientos operativos fueron reconvenidos con los usuario para evitar posibles incumplimientos a la Política de Seguridad de la Información. La siguiente es la distribución porcentual de los correos enviados:



La siguiente tabla expone que tipos de incidentes presentados durante el trimestre, los cuales potencialmente podrían afectar la entidad en su compromiso de preservar la Política de Seguridad de la Información:

Clasificación de incidente	Cantidad
Incidentes Altos	4
Incidentes Medios	3.823
Incidentes Bajos	20
Total	3.847

El grupo de Seguridad de la Información de la Oficina Asesora de Gestión del Riesgo, revisa los incidentes referentes a envío de información sin los controles de seguridad requeridos y los accesos a Internet con contenido de entretenimiento, para analizar la afectación que tienen dentro de los recursos informáticos de la Entidad, concluyendo que no presenta riesgo para nuestros sistemas de información pero si incumplimiento a nuestra política de Seguridad de la Información y no dejan de ser relevantes para tener en óptimas condiciones el uso de los recursos de la entidad como lo es el ancho de banda lo cual dificulta las labores de la Entidad.

El incremento elevado de los eventos de nivel medio reportados por la herramienta OSSIM obedecen al aumento de los niveles de afinamiento de la herramienta DLP y al acceso a YouTube, debido al elevado número de eventos reportados, se tomó la determinación de controlar el uso de internet a los usuarios de la Entidad.

El seguimiento mediante la herramienta DLP, mejora las prácticas y contribuye a seguir los parámetros de la política de la Seguridad de la Información, por lo tanto la gestión de incidentes con respecto al tema se tramitara de manera constante con el fin de garantizar el buen uso de los elementos de la organización.

Así mismo durante el trimestre se efectuó el análisis de log´s de auditoría de la herramienta Soloaudi al sistema de información GA2, determinando que no se presentaron vulnerabilidades en el sistema.

Monitoreo y Seguimiento, de todos los eventos y alarmas que previenen la detección de intrusos, hackers, virus y correo mal intencionado.

Por medio de diferentes herramientas para monitorear el tráfico de la red se logra advertir en tiempo real la presencia de virus, ataques, transito de código malicioso y/o diferentes espectros de código sospechosos. Gracias a estas visualizaciones se puede determinar la fuente de este tipo de elementos para tomar acción de remediación inmediata.

Durante este trimestre la Oficina Asesora de Gestión del Riesgo a través del Grupo de Seguridad de la Información, generó cuatro opciones de mejora que se reflejaron en ajustes que la Oficina Asesora Informática hizo a la plataforma tecnológica de la entidad, evitando con esta acción posibles penetraciones externas.

Sistema de SOC (Security Operation Center)

El estudio de Logs de auditoría generados por nuestro SOC (Security Operation Center) está basado en la herramienta OSSIM de correlación de eventos de Seguridad de la información que Wexler S.A.S adaptó, ajustó y personalizó a las necesidades de CAPROVIMPO, ésta herramienta nos permite rápidos análisis y seguimientos a eventos que puedan afectar la seguridad tanto en nuestra sede principal como en varios puntos remotos (Cali, Medellín, Barranquilla, Ibagué, Bucaramanga, Cartagena, Venecia y Girardot) de Caprovimpo.

Durante el trimestre se detectaron potenciales ataques a nuestra red, en los cuales se observó varias conexiones sospechosas que al revisarlas se trataban de un malware y spyware las cuales fueron mitigados por el Centro de Servicios. No existió para este trimestre ningún ataque efectivo contra nuestra plataforma.

Seguimiento de análisis de vulnerabilidades de la infraestructura tecnológica de la Entidad.

Durante el trimestre se analizaron las vulnerabilidades de criticidad alta que se detectaron las cuales obedecen a dos factores: la carencia de un ”parche” de seguridad en uno de los servidores Windows y a ejecución de un ataque de denegación de servicios por parte del equipo de seguridad de la información; la

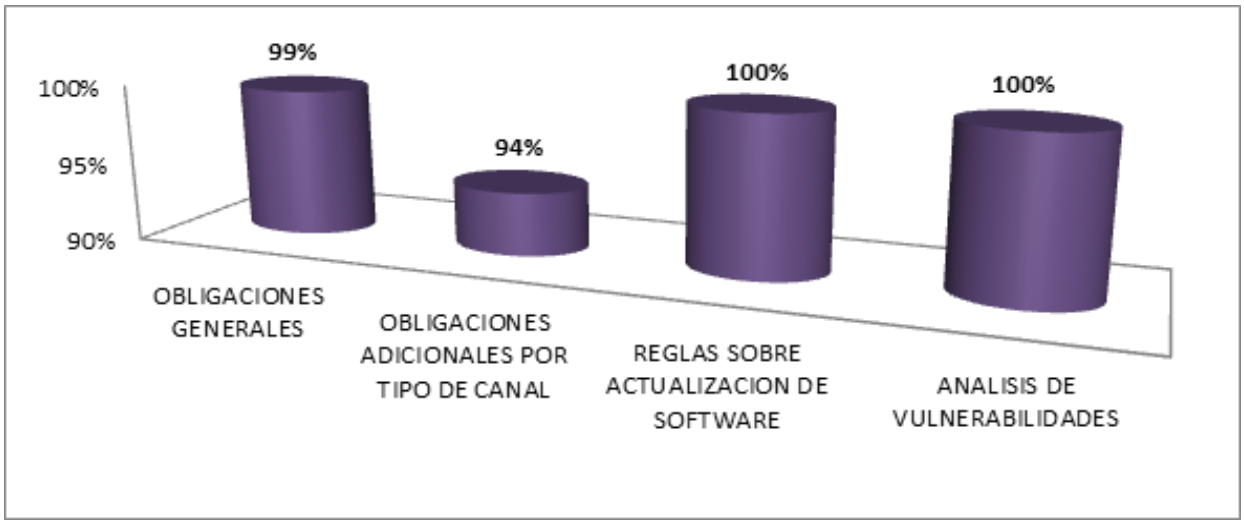
maquina afectada ya fue parchada y se están generando controles y alarmas específicas para mitigar el riesgo del ataque de denegación de servicios. Debido a su complejidad técnica no es posible su total eliminación.

De la misma manera al final del trimestre se incluyó en el análisis de vulnerabilidades la de las aplicaciones web accesibles a través de la red interna. Se inicia el seguimiento al cierre de las mismas y se genera un plan de remediación para que sea ejecutado por la Oficina Asesora Informática.

Seguimiento al cumplimiento de la Circular Externa 052 de 2007 de la SFC

La gráfica reporta el seguimiento trimestral de la Circular 052, en donde se verifica el cumplimiento de los siguientes ítems:

ITEM	CUMPLIMIENTO
Obligaciones generales	99%
Obligaciones adicionales por tipo de canal	94%
Reglas sobre actualización de software	100%
Análisis de vulnerabilidades	100%



En cuanto al tema de Obligaciones adicionales por tipo de canal, el cual se encuentra en un 94 % de cumplimiento, se tienen controles y revisiones actuales por puntos tales como:

Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deberán ser conservadas por lo menos un (1) año o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

Actualmente se trabaja mancomunadamente entre el personal de Seguridad de la Información y el encargado de la implementación del CCTV, cuya operación se está implementando en Bogotá y para el total de los puntos de atención a finales del año en curso.

No se cuenta con cifrado de tráfico en las oficinas Florencia, Cartagena e Ibagué.

En cuanto al tema de Obligaciones generales, en el numeral 3.1.20 de la citada circular no todos los puntos de atención cuentan con las facilidades de acceso exigidas para el personal discapacitado.

Inducciones y capacitaciones.

Se realizó inducción de la normativa y políticas de seguridad de la información a todos los funcionarios y colaboradores que ingresaron en este trimestre 116, contando con la presencia adicional de contratistas de la Entidad, para un total de 121 asistentes.

Inducción	Funcionarios Capacitados	Calificación Promedio
OCTUBRE	3	7.5
NOVIEMBRE	87	8.5
DICIEMBRE	31	9.0

Por parte del Grupo de Seguridad de la Información, se concientiza a todo el personal de la Caja Promotora de Vivienda Militar y de Policía, acerca de las prácticas para el buen manejo de los recursos asignados y los riesgos a los cuales se encuentran expuestos si se hace un mal uso de las herramientas disponibles.

Desde el mismo momento de la capacitación se evidencia un porcentaje alto de importancia en cuanto al tema, no solo por los resultados arrojados en la misma, sino por el manejo que se da en el transcurso de las labores cotidianas y en los diferentes cargos que desempeñan cada uno de los funcionarios. Esto revela de manera concreta el compromiso y el sentido de pertenencia con la entidad y lo expuesto en el tema de Seguridad de la Información.

Acompañamientos especiales y proyectos específicos

Implantación SGSI Certificación 27001

Se continuo con el proyecto de certificación en La Norma Internacional 27001:2005 de Seguridad de la Información a cargo de la Firma Wexler S.A.S. Al cierre del tercer trimestre se llevó a cabo el análisis y conocimiento de los procesos en los cuales intervinieron las áreas de Afiliaciones, Pagaduría, Administración de aportes y Cesantías, en donde se obtuvo el conocimiento de los procedimientos concernientes a cada una de las dependencias, se identificaron y se definieron los riesgos involucrados

dentro de la operación, se calificó el nivel de probabilidad, impacto y criticidad de cada uno de los riesgos con la presencia de cada uno de los líderes de los procesos.

A su vez con la cooperación de la Oficina Asesora de Gestión del Riesgo, se estudió y se redactó los controles presentes en la Entidad, los cuales intervienen de manera constante apoyando cada uno de los procesos y el desarrollo de las actividades cotidianas. Seguido de esto se determinó y se diseñó un esquema general con una definición clara del proceso a seguir, el cual corresponde al plan de tratamiento para mitigar los posibles riesgos que se pueden materializar.

De la misma manera se ha contado con la aprobación y supervisión de la Gerencia General, para la definición y creación de la política de seguridad de la información, la cual se ha puesto en práctica y en medio del proceso de la certificación se divulgará a todo el personal de la Entidad para su conocimiento.

Acompañamiento PCN

El Grupo de Seguridad de la Información ha efectuado el acompañamiento a la implementación del nuevo contrato con CLARO para dar continuidad al PCN .Dentro de estos procesos se efectúo la revisión del estudio previo en cuanto a verificación de la inclusión de todos los puntos requeridos en la Circular 052 de la SFC, así como recomendaciones de tipo técnico y generación de opciones de mejora. Validación técnica de la solución elegida por la entidad y seguimiento al proceso de implementación.

Al cierre de este trimestre se han efectuado 5 reuniones junto con la Oficina Asesora Informática y el proveedor encargado de la implementación (CLARO), se han efectuado dos pruebas de validación de copia de información al centro alterno. Se validó la copia de seguridad de los 13 sistemas de información críticos seleccionados por la entidad al centro alterno de datos de acuerdo con el análisis de riesgos efectuados; de los cuales 12, al cierre de este trimestre, cuentan con una copia en el centro alterno de datos y se definió una estrategia para el aplicativo FÉNIX que debido a la tecnología que utiliza (Win 2008 Server) no cuenta con replicación automática para lo cual la Oficina Asesora Informática efectuará la actualización con la colaboración del proveedor del sistema de información FÉNIX.

Portal Transaccional

El Grupo de Seguridad de la Información ha generado las recomendaciones mínimas de seguridad con que debe contar el nuevo portal transaccional de la entidad; de la misma manera se han efectuado hasta el momento del cierre del cuarto trimestre de 2013, 2 análisis de vulnerabilidades sobre el portal actual el cual es la base del portal transaccional generando las recomendaciones para cada análisis. Se tienen dispuestos y diseñados el plan de pruebas y los procedimientos necesarios para la revisión del

nuevo portal transaccional tan pronto como se tenga el desarrollo listo por parte de la Oficina Asesora Informática.

Validación de licenciamiento

Durante el último trimestre de 2013, se efectuó seguimiento detallado al inventario de software con el que cuenta la Entidad comparado con la cantidad de licencias en uso (inicialmente de Microsoft que es más del 90 % de nuestra plataforma) para este análisis se tomó como materia prima un análisis "SAN" inicial efectuado por Microsoft a solicitud de la Oficina Asesora Informática, el inventarió físico con que cuenta la Entidad y la ejecución de dos análisis de inventarios efectuados a través de herramientas sistematizadas del grupo de seguridad de la información. Definiendo la estrategia de licenciamiento para el 2014 a cargo de la Oficina Asesora Informática.

Por parte de la Oficina Asesora de Gestión del Riesgo a través del Grupo de Seguridad de la Información se realizara seguimiento trimestral al cumplimiento de la legalización de Software de la Entidad.

ESPERANZA CHARRY QUINTERO
JEFE OFICINA ASESORA DE GESTIÓN DEL RIESGO

Proyectó y Elaboró:
Eco. Yakeline Prieto Ballesteros
Profesional Especializado 1 OAGRI