Bogotá, 21 de abril de 2014

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO -SARO-
INFORME I TRIMESTRE DE 2014

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.

De tal modo que para el primer trimestre del 2014, 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 enero y marzo del 2014, 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 107 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	3	97	100
Fallas tecnológicas	0	5	5
Eventos externos	**0**	**2**	**2**
TOTAL	**3**	**104**	**107**

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 84 registros de PNC durante el primer trimestre del 2014, distribuidos como sigue:

Proceso	Producto No Conforme
Sistema de Atención al Consumidor Financiero -SAC-	13
Grupo de Cuentas Individuales	22
Grupo de Cesantías	20
Servicio al Afiliado y Puntos de Atención	29
Total	**84**

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

Durante el trimestre se desarrolló la política de continuidad del negocio la cuál fue presentada al comité de riesgos y recomendada por éste para aprobación en la Junta Directiva en el II trimestre de 2014.

Se recibió por parte de la firma Telmex la primera versión del informe de análisis de impacto del negocio (BIA), el documento definición de estrategias para la recuperación, el cual está siendo evaluada conjuntamente con la Oficina Asesora de Informática.

Se realizó el taller de análisis de impacto BIA con los líderes de los procesos de Cuentas Individuales, Identificación, Afiliación y Gestión del Trámite, Administración de Cuentas Individuales y Cesantías, Gestión Finanzas y Gestión de Riesgos, dicho taller fue dictado por el Ingeniero German Vargas Pedroza de la firma Telmex Colombia.

Se realizaron los primeros simulacros técnicos obteniendo como resultado un 95% en dichas pruebas.

La Oficina Asesora de Gestión del riesgo realizó las siguientes actividades en el punto alterno de continuidad, encontrando los siguientes aspectos:

- Actualmente se encuentran instaladas 2 cámaras de vigilancia, las cuales se encuentran a prueba y seguimiento. Estas se adecuaron paralelamente con las instaladas en la sede principal de CAPROVIMPO y estarían operando satisfactoriamente a finales del mes de Marzo.

Se recomienda revisar la instalación de nuevas cámaras que brinden una mayor visualización tanto en el primer y segundo piso del punto de atención, y validar que su funcionamiento sea óptimo ante cualquier incidente de seguridad.

- Se observa que los extintores se encuentran con fecha de recarga actualizada (Diciembre 2014). De acuerdo a esto se puede garantizar su buen uso ante un caso de un incidente (conato de incendio).

- Racks de comunicación de voz y datos: En operación. Funcionando correctamente. Se encuentran en buen estado de mantenimiento y limpieza. Todos los puntos habilitados funcionando correctamente.

- Ups: En operación. Funcionando correctamente.

- Aire acondicionado: En operación. Funcionando correctamente.

- Cuarto de comunicaciones: Se encuentra en buen estado de mantenimiento, limpieza e iluminación.

- Se evidencio que la infraestructura de RED se encontraba disponible en la mayoría de los puntos de conexión ya que no presentaron inconvenientes de acceso.

- El sistema de comunicación funciono perfectamente a nivel interno y externo.

- A su vez se cuenta con 2 lectores de código de barras, 5 teléfonos (2 en sala de juntas) y 1 fax en correcto funcionamiento.

a) Perfil funcionario:

Se verificó el inventario de equipos disponibles en caso de contingencia, y se aplicaron las pruebas para el ingreso a los siguientes aplicativos, los cuales fueron exitosos:

- INTRANET
- ISOLUCION
- SAC
- GPN

- FOLIUM
- SIE
- KACTUS
- SEVEN
- VIGIA
- GA2
- LEGIS
- HP SERVICE

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 primer trimestre de 2014, brindó inducción a 33 funcionarios que ingresaron a la Entidad y capacitación a 174 funcionarios de los diferentes procesos tal como se muestra a continuación:

Mes	Funcionarios Capacitados	Calificación Promedio
Enero	33	90.45
Febrero	114	96.19
Marzo	60	97.19

SEGURIDAD DE LA 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.

Durante el I Trimestre de 2014, en el caso del correo electrónico, se evidencio un total de 1.211.572 correos distribuidos de la siguiente manera:

Nombre Cuenta	No. Correos	Participación
Caprovimpo	1,082,156	89.32%
Caprovimpo.local	3,182	0.26%
Otros corporativos	107,409	8.87%
Grupo Verytel	2,705	0.22%
Gmail	5,587	0.46%
Hotmail	6,558	0.54%
Synapsis-it.com	3,975	0.33%
Total	**1,211,572**	**100%**

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 usuarios para evitar posibles incumplimientos a la Política de Seguridad de la Información.

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, música, pornografía entre otros, para analizar la afectación que tienen dentro de los recursos informáticos de la Entidad, resultado de la revisión durante este trimestre se generó un informe de evento de seguridad informática al respecto y diferentes recomendaciones verbales con funcionarios involucrados en eventos menores.

Los eventos encontrados durante este período tienen influencia dentro del marco de la unidad de negocio de la Caja Promotora de Vivienda Militar y de Policía, ya que afectan las condiciones y el uso de los recursos de la entidad como lo es el ancho de banda de internet para las labores de la Entidad.

Las Medidas ejecutadas para gestionar que estos incidentes se minimicen en un gran porcentaje, han sido la programación de capacitaciones al personal de CAPROVIMPO dirigido por la Oficina Asesora de Gestión de Riesgos, validación y restricción de Internet completo según perfiles labores asignados y monitoreo por medio de las herramientas disponibles al tráfico de la red y segmentación de la misma.

Así mismo, se efectuó el análisis de log´s de auditoría de la herramienta Soloaudi al sistema de información GA2, detectando los siguientes movimientos:

- Creación de 8 usuarios con privilegios, se efectuó la solicitud al líder de Operaciones y se pudo validar que cuenta con el debido formato para sustentar estas adiciones y su respectiva autorización.

- El área de operaciones reportó que las tablas de clientes y movimientos, cuentan con modificaciones diarias que se generan por medio de la líder del proceso Jaqueline Buitrago, quien valida el registro a modificar según las solicitudes o registros de los afiliados. Todos estos parámetros reposan en el sistema con la información detallada de las ejecuciones realizadas los cuales se encuentran disponibles para su consulta cuando se requieran. Por parte del grupo de Seguridad de la Información se dispone un seguimiento conjunto con el grupo de operaciones semanal para el análisis de modificaciones que se requieran según el proceso.

- Se verificó con el grupo de servicio al afiliado según el reporte generado y expuesto en la tabla de cuentas, las modificaciones realizadas según el análisis y proceso que se lleva a cabo en la dependencia. Los cambios reflejados en los meses de enero, febrero y marzo se deben a que el outsourcing contratado termina su contrato y se procedió con la des habilitación de los usuarios en uso. De igual manera todos los reportes reposan en el sistema.

Por tanto, el grupo de Seguridad de la Información hace seguimiento semanal para el análisis de nuevos eventos y modificaciones efectuadas en las tablas de cuenta que reportan cambios.

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

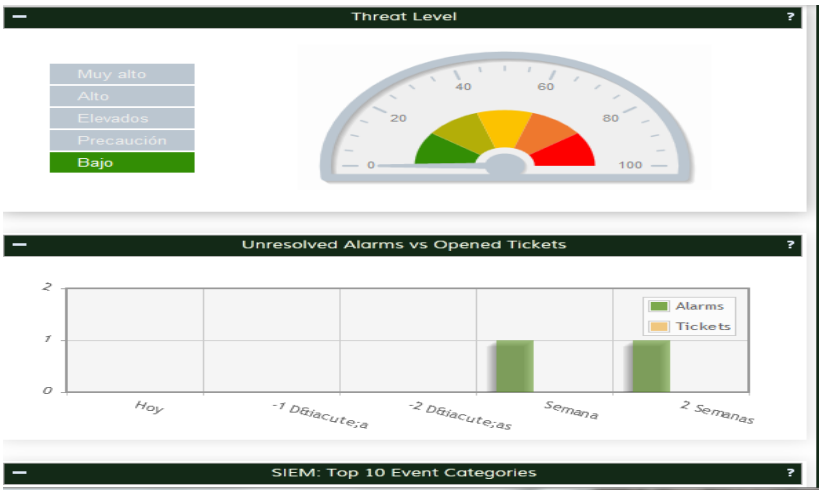
Por medio de diferentes herramientas para monitorear el tráfico de la red se logra advertir en tiempo real la presencia de virus, ataques, transito de código malicioso y/o diferentes espectros de código sospechosos. Gracias a estas visualizaciones se puede determinar la fuente de este tipo de elementos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

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.

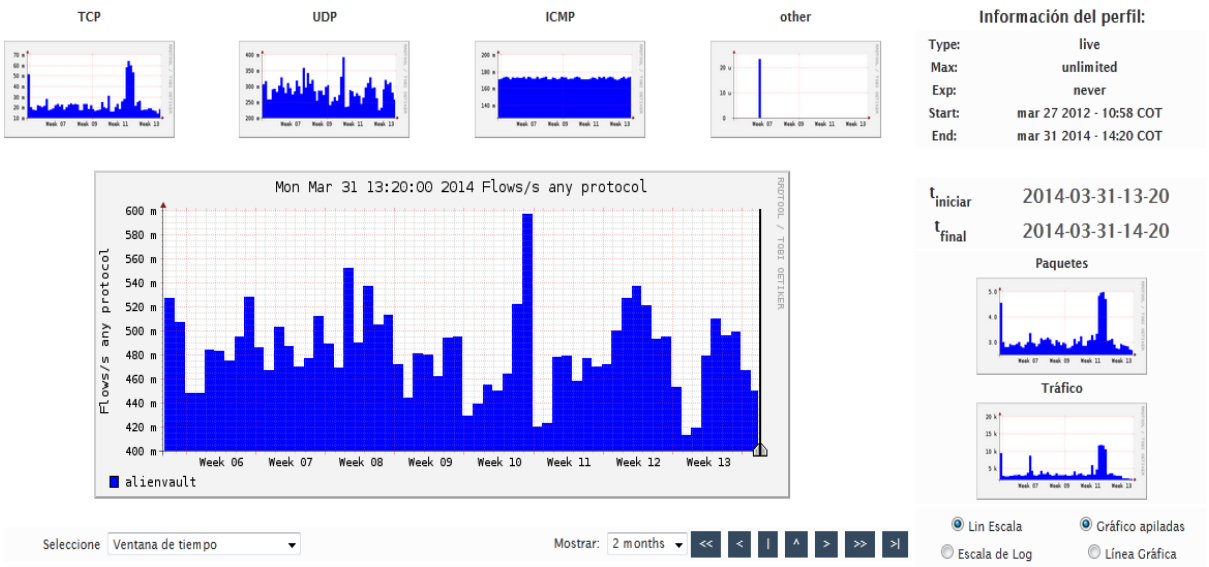
De este seguimiento se generaron las siguientes estadísticas:

La siguiente gráfica evidencia que durante el I trimestre 2014 no se presentaron amenazas que pudieran afectar la infraestructura tecnológica de la entidad.



Se efectuó un completo y permanente análisis de tráfico, que salvo ataques planificados, especializados, elaborados y ejecutados por el grupo de seguridad de la información no se presentaron alteraciones (de estos ataques específicos que generan

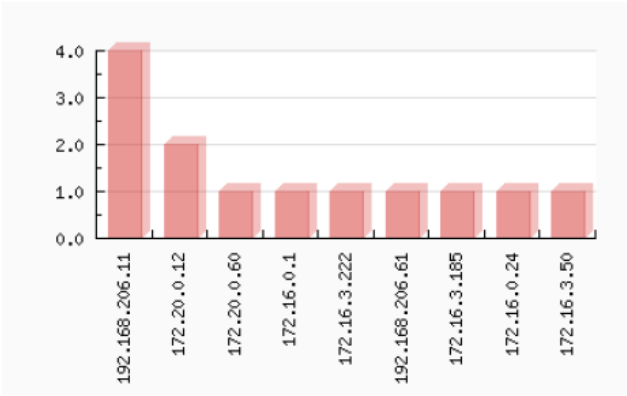
un incremento en la semana 10 de la gráfica se generó una vulnerabilidad la cual se reporta en el aparte "Vulnerabilidades" del Presente informe)



Adicionalmente, el Grupo de seguridad de la información de la Oficina Asesora de Gestión del Riesgo monitorea permanentemente mediante las diversas herramientas de OSSIM, posibles firmas maliciosas o comportamientos no estándar en toda la infraestructura especialmente del segmento de servidores.

Reporte de Alarmas - Top 10 equipos atacantes Desde: 2014-01-01 a: 2014-03-31

Equipo	Ocurrencias
Host-192-168-206-11	4
alienvault	2
Host-172-20-0-60	1
172.16.0.1	1
Host-172-16-3-222	1
Host-192-168-206-61	1
172.16.3.185	1
Host-172-16-0-24	1
172.16.3.50	1



Todas las firmas reveladas durante este período, fueron generadas por el Grupo de Seguridad de la Información de la Oficina Asesora de Gestión del Riesgo como parte del proceso permanente de ejecución de pruebas de penetración y Ethical hacking.

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

Durante este período fue posible acceder a infraestructura crítica de la entidad ubicada en el data center de triara mediante el uso de elaborados ataques informáticos ejecutados de manera controlada por el grupo de Seguridad de la Información de la Oficina Asesora de Gestión del Riesgo. Dichos ataques fueron reportados de manera inmediata a la Oficina Asesora de Informática con su respectivo informe de Gestión de Incidentes de Seguridad de la información y las correspondientes recomendaciones de cierre y el acompañamiento requerido para su toma de acción.

Es importante resaltar que el 90% de las vulnerabilidades detectadas durante este periodo hacen referencia a la implementación de nuevos computadores, nuevas herramientas, la implementación de Nuevo PCN, cambio y salida de tres contratistas de la entidad.

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

En la siguiente tabla reporta el seguimiento trimestral de la Circular 042 de 2012, en donde se verifica el cumplimiento de los siguientes ítems:

Item	Cumplimiento
2.15 Autenticación	100%
2.16 Mecanismos fuertes de autenticación	100%
2.18 Proveedores redes y servicios de telecom.	60%
3.1 Seguridad y calidad	99%
3.2 Tercerización y outsourcing	100%
3.3 Documentación	100%
3.4 Divulgación de información	100%
4.1 Oficinas	97%
4.7 Centro de atención telefónica	100%
5. Reglas sobre actualización de software	100%
7. Analisis de vulnerabilidades	100%

Por otra parte, el tema de Proveedores de Redes y Servicios de Telecomunicaciones, se encuentra en un 60 % de cumplimiento y describe lo siguiente:

- *Empresas reguladas por la Comisión de Regulación de Comunicaciones y debidamente habilitadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, responsables de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros (de acuerdo a lo establecido en la resolución 202 de 2010 art.1).*

Actualmente, se solicitó a los proveedores por medio de la Oficina Asesora de Informática, los acuerdos de niveles de servicio y el cumplimiento de lo pactado para su verificación y correspondiente comprobación.

El tema de Seguridad y Calidad se describe lo siguiente:

- *Considerar en sus políticas y procedimiento relativos a los canales y medios de distribución de productos y servicios, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.*

En validación con el Ing. Jorge Caicedo, actualmente, el único punto dispuesto con todas las adecuaciones para acceso a discapacitados es el de la Ciudad de Cali, para los demás sitios de atención se sigue con la gestión por parte del área administrativa de la compra de locales para adecuar de manera correcta conforme con lo solicitado en la norma.

Del numeral de Oficinas se tiene lo siguiente:

- *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.*

Se confirma con el Mayor Jorge Iván González, la entrega de las Cámaras de la sede principal y de Venecia en su total funcionamiento. A partir de la fecha se entra en estudio de mercadeo para la realización de estudios previos y futura contratación para los puntos de atención.

- *La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de Gateway, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.*

El Ing. Jose Canan, reporta que se firmó con la empresa Evolution la implementación por 14 meses del estudio de las utm's actuales y la que se encuentra pendiente en la sede de Florencia. Se estará realizando acompañamiento a esta implementación para revisar fechas y procesos para llevar a buen término esta instalación.

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 el mes de Enero, contando con la

presencia adicional de contratistas de la Entidad, para un total de 28 asistentes y capacitación a 266 funcionarios de los diferentes procesos.

Mes	Funcionarios Capacitados	Calificación Promedio
Enero	28	93.21
Febrero	114	96.19
Marzo	60	97.19

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 continuó 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 primer 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.

Se inició el desarrollo del nuevo manual de Seguridad de la Información, teniendo en cuenta la reestructuración de la entidad y el nuevo mapa de procesos, se está

trabajando en adaptar las labores ya desarrolladas, a partir de las nuevas caracterizaciones y procedimientos.

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 13, 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 efectuó la copia manual al centro alterno de datos y se cuenta con un Back up de la información pero no replica en tiempo real.

Durante dos fines de semana se ha acompañado el proceso de ejecución de pruebas técnicas para validar el proceso de copia y replicación. En esos tres primeros días de pruebas se pudo configurar, afinar y validar la efectividad del plan de continuidad para los aplicativos GA2, Seven, Vigia, Dialogo, Orion, soluaudit, Sac, monitoreo y control.

Se tiene programado para el próximo trimestre las pruebas funcionales y pruebas de Vulnerabilidades

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 primer trimestre de 2014, 2 análisis de vulnerabilidades sobre el portal actual el cual es la base del portal transaccional generando las recomendaciones para cada análisis. Se tiene dispuesto y diseñado 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 primer trimestre de 2014, 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.

Dichos análisis presentaron unas diferencias de cumplimiento los cuales fueron presentados a la gerencia General por parte de la Jefe de la Oficina Asesora de Gestión del Riesgo en tres mesas de trabajo, en conjunto con el Jefe de la Oficina Asesora de Informática. Está pendiente la compra del GAP de licenciamiento de acuerdo con los anteriores análisis realizados y la confirmación por parte de la Firma Microsoft de la obligación de la Entidad de estar al día en su legalización del licenciamiento usado. Se culminó este proceso generándose la respectiva orden de compra para el cumplimiento de esta obligación. Para el Segundo periodo se tiene contemplado ampliar el alcance para abarcar el software y licenciamiento no Microsoft.

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.

El Grupo de Seguridad de la Información presenta las principales conclusiones de su gestión durante el primer trimestre del 2014:

De acuerdo con el alcance que ofrece el análisis de vulnerabilidades, la infraestructura tecnológica de la Caja Promotora de la Vivienda Militar y de Policía presenta un nivel se seguridad acorde con las exigencias regulatorias y adecuado para la ejecución normal de su operación pero es muy importante tomar acción inmediata de las nuevas vulnerabilidades detectadas.

Debido a una vulnerabilidad de tipo de estalación de privilegios se pudo comprometer parte de la infraestructura alojada en el data center de Triara utilizando técnicas de lata complejidad técnica. Esta vulnerabilidad fue atendida de manera inmediata y se configuraron controles adicionales para minimizar el riesgo de explotación de esta vulnerabilidad y como medida definitiva la plataforma afectada será retirada de operación para el siguiente trimestre.

Se continuara el acompañamiento por parte del Grupo de Seguridad de la Información para el proyecto del Portal Transaccional, con el fin de asegurar la plataforma y las consultas que se generan hacia las bases de datos.

Se cuenta con una disponibilidad de la plataforma informática superior al 97% durante el primer trimestre de 2014 y 0 ataques efectivos a la plataforma, disponibilidad de Correo 97.0%, Directorio Activo 99.2%, Plataforma GA2 97.1%, Plataforma DIALOGO 97.3%, Plataforma FOLIUM 97.97%, Intranet 96.9%.

El 2.7% consolidado de no disponibilidad de la plataforma obedeció a ventanas de mantenimiento programadas por la entidad en tiempos no laborales y fines de semana, en días ordinarios después de las 8pm, y tres días de labores de pruebas técnicas programados (fin de semana) para el nuevo PCN (Plan de Continuidad del Negocio).

ESPERANZA CHARRY QUINTERO
JEFE OFICINA ASESORA DE GESTIÓN DEL RIESGO

Proyectó y Elaboró:
Mayra Montenegro
Profesional Especializado 1 OAGRI