Bogotá, 10 de julio de 2014

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO -SARO-

INFORME II 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.

Durante el II trimestre de 2014 se realizó revisión a los riesgos operativos asociados a cada proceso, en mesas de trabajo la Oficina Asesora de Gestión del Riesgo con los líderes de cada proceso realizaron una revisión detallada a la matriz de riesgos, causas y a los controles implementados, realizando ajustes en las causales de los mismos e implementando nuevos controles en algunos casos. Se mantiene 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.

Se realizó la entrega de una carpeta a cada uno de los Subgerentes, la cual contiene:

- Mapas de riesgos operativos de cada uno de los procesos involucrados con la Subgerencia.

y a cada líder de los procesos, la carpeta que contiene:

- Acta de la reunión realizada entre la OAGRI y los líderes de cada proceso, donde se realizó revisión detallada a la matriz de riesgos y se ajustaron causales y controles.
- Matriz y mapa de riesgo con los cambios realizados.
- Matriz de riesgos asociados al plan anticorrupción.
- Matriz riesgos estratégicos.
- Planillas de asistencia a la capacitación realizada por la OAGRI a los funcionarios de cada proceso.

AJUSTE Y ACTUALIZACIÓN DEL MANUAL

Con la firma Pronus se realizó una revisión y ajuste de la metodología para la identificación, medición, control y monitoreo de los riesgos operativos los cuales quedan consignados en el manual que se está actualizando. Será publicado en ISOLUCION una vez sean aprobados por la Junta Directiva

REGISTRO DE EVENTOS DE RIESGO OPERATIVO -RERO-

Durante el periodo comprendido entre abril y junio 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 158 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	2	152	154
Fallas tecnológicas	0	3	3
Daños a activos fijos	0	1	1
TOTAL	**2**	**156**	**158**

Uno de los eventos de perdida fue dictado en la resolución 252 de 2014, pago sentencia del Tribunal Contencioso Administrativo de Risaralda dentro del proceso 2011-00042 por concepto indexación $2.691.578 y el % moratorio $1.813.840 del afiliado. Jhon James Ayala Correa cc-18.597.726 rads-20140083095 y 20140070534 para un total de $4.505.418. Igualmente, se presentó el evento de riesgo dictado en resolución 229 de 2014 compensación por rompimiento equilibrio financiero de contrato 21-1992 con la Constructora Codinem Ltda. por valor de 683mill aprox, en cumplimiento condena por fallo judicial en 2° instancia de 16 ago-2012 del consejo estado a orden del juzgado 1 laboral circuito Bogotá, a través depósito judicial radicado -20140085074 por valor de $214.458.85 correspondiente a un saldo pendiente por pagar del total de la sentencia.

PRODUCTO NO CONFORME

Como insumo para la identificación de riesgos, se lleva a cabo el control estadístico del Producto No Conforme –PNC-. El Proceso Gestión del SAC, el Proceso Administración de Cuentas Individuales y Cesantías, el Proceso Identificación, Afiliación y Gestión del Trámite con sus Puntos de Atención reportaron 148 registros de PNC durante el segundo trimestre del 2014, distribuidos como sigue:

Proceso	Producto No Conforme
Gestión del SAC-	14
Administración de Cuentas Individuales y Cesantías	28
Identificación, Afiliación y Gestión del Trámite	106
Total	**148**

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 ANTICORRUPCIÒN Y ATENCIÒN AL CIUDADANO

Con el fin de dar cumplimiento con la Ley 1474 de 2011, CAPROVIMPO revisó la estrategia de lucha contra la Corrupción en el Plan Anticorrupción y de Atención al Ciudadano, el cual es un instrumento de tipo preventivo para la gestión de la Entidad. Se realizó una segunda versión del manual el cual fue revisado por la Subgerencia de Atención al afiliado y operaciones, líder de Gestión del SAC, líder de Servicio al Afiliado, profesional especializado 2 Grupo Aseguramiento del servicio y la Oficina Asesora de laneación.
Así mismo se revisaron los riesgos con los 16 líderes de los procesos y se socializaron con todo el personal de planta.

Teniendo en cuenta la efectividad de los controles sobre los Riesgos Operativos, que incluye los riesgos de corrupción 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, lo cual nos permito observar que se dio cumplimiento con la meta establecida para el segundo trimestre de 2014.

PLAN DE CONTINUIDAD DEL NEGOCIO

Durante el II Trimestre de 2014, la Oficina Asesora Gestión del Riesgo (OAGRI), realizó seguimiento al desarrollo del contrato firmado con la firma TELMEX, el cual se constituye como un Sistema de

Continuidad de Negocio que permite establecer, operar, monitorear, mantener, mejorar las medidas preventivas y capacidad para seguir operando el negocio, aun cuando ocurra un evento que interrumpa procesos y funciones críticas. Mediante este, CAPROVIMPO ha aplicado procesos proactivos que permiten prepararse y definir estrategias coordinadas para responder a eventos que puedan afectar la continuidad de negocio donde se incluya administración de crisis, planes de contingencia y capacidad de retorno a la operación normal.

En relación a la supervisión funcional del PCN, la OAGRI presenta dos roles específicos dentro de la prueba:

a) En primer lugar como observador de la misma, donde se busca identificar los posibles riesgos o contingencias que se puedan presentar en un caso real de continuidad.
b) En segundo lugar como funcionarios, donde realizaba las pruebas a los diferentes aplicativos, que se consideran críticos dentro de la organización.

i. Perfil Observador:

Dentro de las diferentes actividades realizadas por los delegados de la Oficina Asesora de Gestión del Riesgo, como observadores se identificaron los siguientes puntos en el PAC de la Entidad:

- Se realizó una prueba piloto en el mes de junio con dos cámaras ip, las cuales estaban siendo monitoreadas desde la sede principal de CAPROVIMPO. Debido al resultado de la prueba piloto fueron deshabilitadas, ya que al realizar el backup este consumía bastante ancho de banda.
- Debido a una falla técnica el DVR se encuentra sin funcionamiento, dado que semanas atrás este se quemó y quedando inservible, ocasionando que las cámaras quedaran fuera de funcionamiento.
- En este momento la sede no cuenta con ningún CCTV en funcionamiento, por este motivo la sede tiene una vulnerabilidad de alto impacto.
  Se recomienda implementar lo más rápido posible un nuevo DVR, para que la sede cuente nuevamente con el sistema CCTV.
- Los computadores que se revisaron no cuenta con ningún tipo de seguridad física, es indispensable que sean asegurados por una guaya, para tener más seguridad y no incurrir en una pérdida de estos equipos.
- 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. 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.
- 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.

Se recomienda lo siguiente de manera general:

- Revisar nuevamente la configuración de la impresora del primer piso en todos los equipos que hacen parte del PAC o en su defecto instalar una impresora en el segundo piso que opere para el plan de Continuidad en caso de contingencia, ya que esta recomendación se ha realizado en los informes anteriores y no se ha efectuado.

Se incumple con los siguientes parámetros:

- El ingreso al PAC se encuentra protegido por una puerta de vidrio, un electroimán el cual activa o desactiva mediante un control de bloqueo o por medio de un dispositivo de identificación dactilar, el

cual en estos momentos se encuentra fuera de servicio, y cualquier funcionario tiene acceso al PAC. La puerta donde se ingresa permanece abierta incurriendo en una falta grave.

- La puerta situada en el cuarto de comunicaciones la cual es habilitada por medio de un dispositivo de identificación, se encuentra fuera de servicio, y esto permite que cualquier funcionario tenga acceso al cuarto de comunicaciones, donde se encuentra el Rack de ETB, CCTV, alarmas y entre otros equipos de comunicación.
- No se tiene ningún registro de las personas que ingresan al PAC, quedando vulnerable el cuarto de comunicaciones.
- El cuarto eléctrico que se encuentra ubicado en el segundo piso y en el primer piso, cuentan con puertas de seguridad, las cuales se encontraron abiertas en su momento.
- En uno de los cuartos eléctricos se encuentra anclada a la pared la cajilla de seguridad (llaves)

ii. Perfil funcionario:

Se verificó el inventario de equipos disponibles en caso de contingencia, se encontraron 12 (doce), identificados con número de serial y cuentan con ingreso solo por clave de administrador. Se debe revisar por parte del personal encargado el ingreso por administrador y por otros usuarios autorizados.

En los equipos restantes se realizaron las pruebas para el ingreso a los siguientes aplicativos:

- Intranet
- Isolución
- SAC
- GPN
- FOLIUM
- SIE
- KACTUS
- SEVEN
- VIGIA
- GA2
- LEGIS
- HP SERVICE
- SYSTEM CENTER SERVICE MANAGER

- Se requiere revisar 2 equipos a los que no se lograron acceder.
- Se observó que no se encuentra instalado el aplicativo DIALOGO en ningún equipo, se recomienda realizar la configuración del aplicativo en mención ya que hace parte de los sistemas de información críticos para el PCN.

Dado lo anterior, se recomienda verificar todos los puntos anteriormente referenciados, para una prueba a futuro del plan de continuidad con el fin de probar la funcionalidad de todos los equipos.

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 segundo trimestre de 2014, brindó inducción a 13 funcionarios que ingresaron a la Entidad y capacitación a 186 funcionarios de los diferentes procesos tal como se muestra a continuación:

Mes	Funcionarios Inducción	Funcionarios Capacitados	Calificación Promedio
Abril	4	0	100
Mayo	5	0	100
Junio	4	186	99.93
TOTAL	**13**	**186**	**99.98**

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

CUENTAS CORREO	NUMERO DE CORREOS
cuenta caprovimpo.gov.co	899.359
cuenta gmail.com	7.015
cuenta hotmail.com	9.384
otros corporativos	109.466

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.

Se han adoptado medidas para evitar la materialización de incidentes con 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 asignados y monitoreo por medio de las herramientas disponibles al tráfico de la red y segmentación de la misma.

Se efectúa el análisis de log´s de auditoría de la herramienta Solo Audi al sistema de información GA2, detectando los siguientes movimientos:

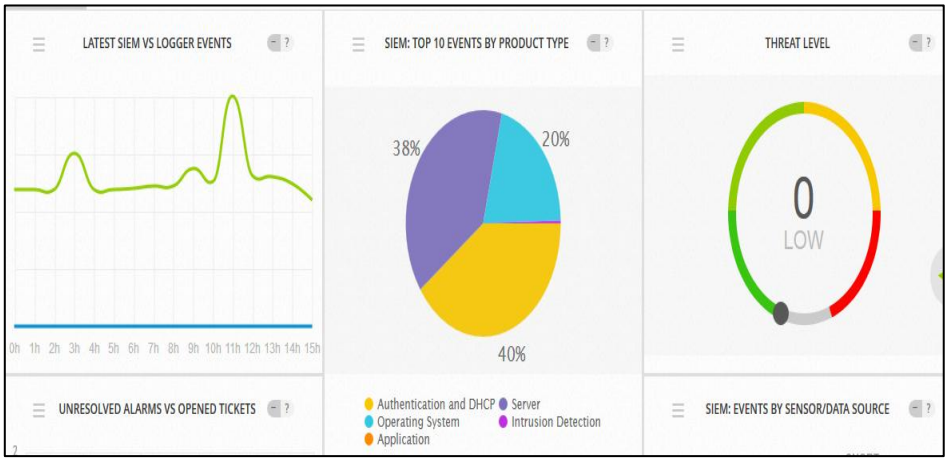
Se monitorea y se hace seguimiento de todos los eventos y alarmas que previenen la detección de intrusos, hackers, virus y correo mal intencionado.

Sistema de SOC (Security Operation Center)

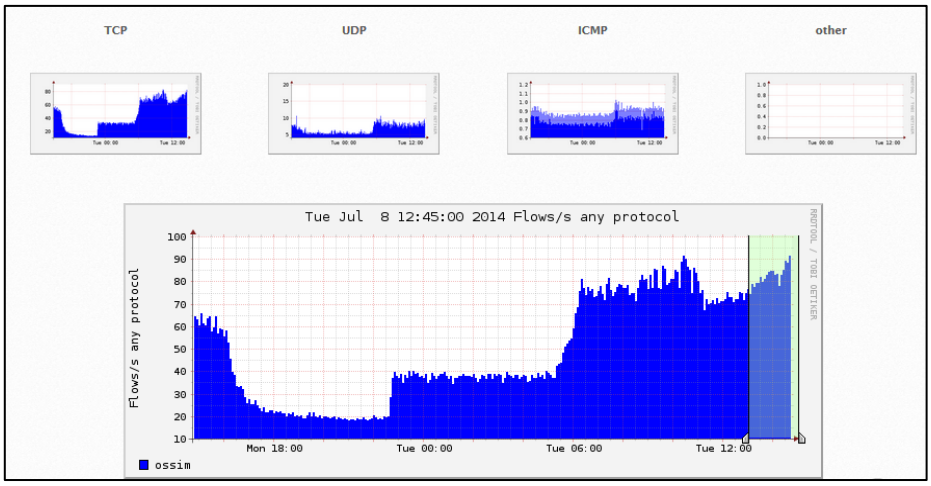
El estudio de Logs de auditoría generados por nuestro SOC (Security Operation Center) está basado en la herramienta OSSIM de correlación de eventos de Seguridad de la información que Wexler S.A.S adaptó, ajustó y personalizó a las necesidades de CAPROVIMPO, ésta herramienta nos permite un rápido análisis y seguimientos a eventos que puedan afectar la seguridad tanto en la 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 II trimestre 2014 toda amenaza fue detectada por el grupo de Seguridad de la información y controladas sin generar riesgos que pudieran afectar la infraestructura tecnológica de la entidad.

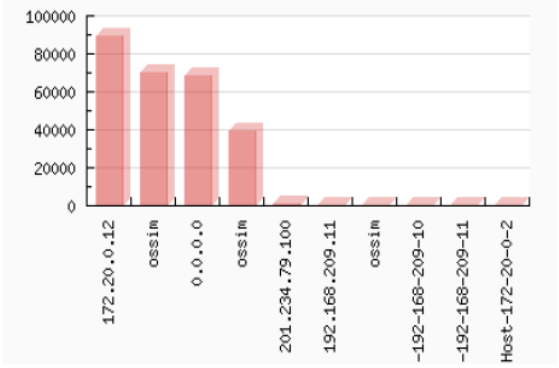


Se efectuó un completo y permanente análisis de tráfico, que salvo ataques planificados, especializados, elaborados y ejecutados por el grupo de seguridad de la información no se presentaron alteraciones.



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.

Host	Occurrences
172.20.0.12	88.845
ossim	70.030
0.0.0.0	67.981
ossim	39.048
201.234.79.100	641
192.168.209.11	110
ossim	76
Host-192-168-209-10	62
Host-192-168-209-11	51
Host-172-20-0-2	48



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

Durante este período fue posible acceder a la infraestructura crítica de la entidad ubicada en nuestras oficinas principales de la cede del CAN mediante el uso de elaborados ataques informáticos ejecutados de manera controlada por parte del 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.

Seguimiento al cumplimiento de la Circular Externa 042 de 2012 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 AUTENTICACION	**100%**
2.16 MECANISMOS FUERTES DE AUTENTICACION	**100%**
2.18 PROVEEDORES REDES Y SERVICIOS DE TELECO	**80%**
3.1 SEGURIDAD Y CALIDAD	**99%**
3.2 TERCERIZACION Y OUTSORCING	**100%**
3.3 DOCUMENTACION	**100%**
3.4 DIVULGACION DE INFORMACION	**100%**
4.1 OFICINAS	**96%**
4.7 CENTRO DE ATENCION TELEFONICA	**100%**
5. REGLAS SOBRE ACTUALIZACION DE SOFTWARE	**100%**
7. ANALISIS DE VULNERABILIDADES	**100%**

De igual forma se confirmó la instalación de más cámaras en el primer piso de la sede principal reforzando la seguridad de las mismas en el área de atención al afiliado y los pasillos de todos los pisos.

- *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.*

La Oficina Asesora de Informática 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.

El numeral de Proveedores redes y servicios de Teleco

Con relación al numeral de la C.E 042 del 2012 numeral 2.18, la Oficina Asesora de Informática está realizando la revisión de la documentación de las compañías prestadoras de servicios de telecomunicaciones en CAPROVIMPO para validar que cumplan con lo establecido en la resolución 202 de 2010 Art.1.

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 abril, mayo y junio, para un total de 13 asistentes. Igualmente, se implementó un plan de cultura en la administración de riesgos asociados a la seguridad de la información mediante el envío semanal de correos "tips" con temas específicos de seguridad, con recomendaciones de uso, reglamentación y actualidad en seguridad de la información.

Mes	Funcionarios Capacitados	Calificación Promedio
Abril	4	100
Mayo	5	100
Junio	4	100

Acompañamientos especiales y proyectos específicos

Acompañamiento PCN

El Grupo de Seguridad de la Información ha efectuado el acompañamiento a la ejecución del contrato con TELMEX para dar continuidad al PCN.

Al cierre de este trimestre se ha efectuado la revisión de la conexión de la entidad al centro alterno se observa que se cuenta con una copia de datos.

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 segundo trimestre de 2014, 3 análisis de vulnerabilidades sobre el portal transaccional generando las recomendaciones respectivas.

Validación de licenciamiento

Se efectuó un análisis del 100% de las máquinas de la entidad tanto en la sede principal del CAN como en cada una de las sucursales desinstalando todo software no autorizado y debidamente licenciado.

Se cuenta con una disponibilidad de la plataforma informática superior al 98% durante el segundo trimestre de 2014 y 0 ataques efectivos a la plataforma, disponibilidad de Correo 98.0%, Directorio Activo 99.2%, Plataforma GA2 98.1%, Plataforma DIALOGO 97.3%, Plataforma FOLIUM 97.97%, Intranet 96.9%.

El 1.9% 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 un día de labores de pruebas técnicas programados (fin de semana) para el nuevo PCN.

INFORME DE ACTIVIDADES PROYECTO DE ALISTAMIENTO PARA LA CERTIFICACIÓN EN EL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN LA NORMA ISO 27001:2013

CAPROVIMPO - GRUPO ÓPALUS

1. Revisión de la documentación actual de los procedimientos de TI en ISOLUCION

Se realizó un análisis de brechas entre los aspectos documentados y los procesos ejecutados en el día a día de la función informática para poder establecer los aspectos que se cumplen y cuáles no, en el contexto de los requisitos de la norma **ISO20000-1** y determinar cómo subsanar cada uno de las brechas encontradas para cumplir.

Los procedimientos analizados fueron los siguientes:

- Gestión de Cambios , gestión de eventos , gestión de Incidentes ,gestión de problemas ,gestión de Accesos ,gestión de ANS, gestión de Red, gestión de capacidad , gestión de Disponibilidad ,gestión de Red ,catálogo de Servicio.

El resultado del entendimiento y la evaluación de los procedimientos en CAPROVIMPO muestran en forma general un nivel de cumplimiento importante en lo relacionado con la alineación de los documentos con **ISO 20000-1** y las mejores prácticas de ITIL. Sin embargo, existe una brecha importante respecto a las actividades implementadas, en algunos casos por que la herramienta para gestión del servicio se encuentra en desarrollo (Service Manager) y en otros casos porque el procedimiento no se ha implementado formalmente.

Se entregó la documentación formal de los procedimientos mencionados en el análisis, para que fueran actualizados en el SGC, previa divulgación y conocimiento de los funcionarios de la Oficina Asesora de Tecnologías de Información.

2. Análisis de Brechas Anexo A ISO 27001: 2013.

Se realizó este análisis para determinar el estado real de la entidad frente a los requisitos del ANEXO A de la Norma Técnica Colombiana ISO27001:2013, por medio de la cual se puede derivar el grado de cumplimiento frente a los requisitos establecidos en dicha norma, así como entender cuáles son las iniciativas que se están llevando a cabo para el cierre de las brechas identificadas y cuales definitivamente requieren un plan de acción sobre cada una de ellas, plan de acción que se sugirió para cada uno de los dominios que conforman el anexo mencionado.

El diagnóstico se llevó a cabo a través de una serie de preguntas realizadas cruzando una lista de chequeo que se realizó con los funcionarios de la Oficina Asesora de Informática de CAPROVIMPO con el fin de lograr un mayor entendimiento de la verdadera situación de la entidad frente a los controles del Anexo A de la norma ISO27001 y de algunos proyectos que ayudarían a ir cerrando las brechas que se pudieren encontrar en su momento establecidas por la actual situación.

El resultado del análisis de brechas de CAPROVIMPO frente al Anexo A de la norma ISO27001:2013 muestra un nivel de desarrollo del 81% y un nivel de riesgo BAJO, lo cual se considera SATISFACTORIO.

3. Identificación de Activos de Información y Gestión de Riesgos asociados.

Para cada uno de los 11 procedimientos relacionados en el numeral 1, se realizaron las siguientes actividades:

- Reunión con el Líder de Proceso
- Identificación de activos y elementos de información con líderes de proceso
- Identificación de riesgos, causas y vulnerabilidades asociados a los activos y elementos de información

- Reunión de validación de activos y riesgos de los elementos de información con líderes de procesos, calificación de riesgos
- Ajuste de matrices de riesgos
- Reuniones de avance de las matrices completas
- Obtención del mapa de riesgo inherente
- Identificación y calificación de controles con el encargado del proceso
- Obtención de mapa de riesgo residual

Del análisis anterior, se identificaron 36 activos de información y 21 riesgos asociados a dichos activos de información con los siguientes riesgos inherentes y residuales:

Tabla 1. Riesgos Identificados y valoración

RIESGOS	DESCRIPCION DEL RIESGO	RIESGO INHERENTE	RIESGO RESIDUAL
RA 1	Daño o mal funcionamiento	Riesgo Alto	Riesgo Menor
RA2	Utilización Errada o Inadecuada	Riesgo Bajo	Riesgo Bajo
RA3	Acceso no autorizado	Riesgo Moderado	Riesgo Menor
RA4	Perdida / Daño	Riesgo Alto	Riesgo Menor
RA5	Ataques externos (hacking no ético)	Riesgo Alto	Riesgo Menor
RA6	Modificación sin autorización	Riesgo Menor	Riesgo Bajo
RA7	Documento No actualizado	Riesgo Menor	Riesgo Bajo
RA8	Mala Gestión del Conocimiento	Riesgo Alto	Riesgo Menor
RA9	Perdida de información acumulada en personal clave	Riesgo Extremo	Riesgo Menor
RA10	Denegación Del Servicio	Riesgo Moderado	Riesgo Menor
RA11	Incumplimiento ANS	Riesgo Alto	Riesgo Menor
RA12	No gestión del requerimiento	Riesgo Menor	Riesgo Bajo
RA13	Diligenciamiento errado y/o incompleto	Riesgo Moderado	Riesgo Bajo
RA14	Ausencia del control en el Inventario	Riesgo Moderado	Riesgo Bajo
RA15	Asignación inadecuada a los Servicios Informáticos	Riesgo Alto	Riesgo Menor
RA16	Incumplimiento de Derechos de Autor	Riesgo Alto	Riesgo Menor
RA17	Insuficiencia de licencias	Riesgo Bajo	Riesgo Bajo
RA18	Errores en la definición del Plan de Capacidad	Riesgo Menor	Riesgo Bajo
RA19	No actualización de la información	Riesgo Moderado	Riesgo Menor
RA20	No actualización de la arquitectura de red	Riesgo Moderado	Riesgo Menor
RA21	Errores en la definición de las Especificaciones	Riesgo Moderado	Riesgo Menor

Según la información de la tabla anterior se puede resumir la participación de categoría de riesgo en las figuras 1 y 2.

Figura 1. Riesgos Inherentes

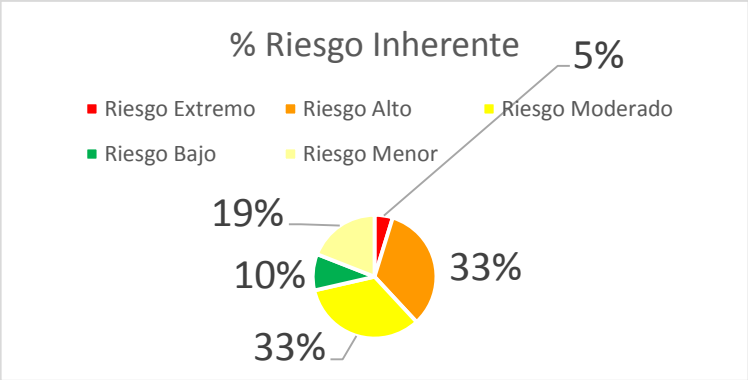
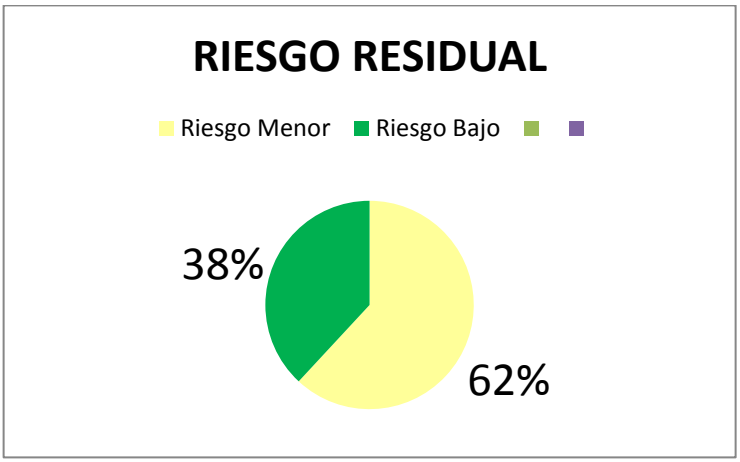


Figura 2. Riesgos Residuales



. Documentación manual de seguridad

Dada la reciente actualización de la norma ISO 27001 a la versión 2013, se realizó la revisión del manual de seguridad, actualizando los requerimientos establecidos en la nueva versión de la norma y de sus Anexos.

La actividad de la revisión se realizó de forma conjunta con las áreas de Riesgos, Tecnología y el Grupo Ópalus.

5. Definición de métricas y medidas para calcular el desempeño del SGSI

Fueron definidas las métricas e indicadores que deberían ser implementados en el SGSI de Caprovimpo, los cuales se encuentran siendo evaluados por parte de la entidad.

6. Culturización

Como parte de la necesidad y requisito indispensable de establecer el SGSI en Caprovimpo, se realizó un proceso de culturización en el cual se hace extensiva a toda la entidad, conceptos de seguridad de la información y la importancia que para todos ellos representa la puesta en marcha de un SGSI para la entidad.

Se han realizado cuatro sesiones de sensibilización, donde se han invitado a todos los funcionarios de la entidad.

7. Porcentaje de Avance y Pasos a Seguir

El avance del proyecto es del 80% respecto a lo programado, sin retrasos en el cronograma.

Los pasos a seguir son:

- Entrega del tratamiento de los riesgos de los activos de información
- Auditoría de Primera parte para medir el grado de cumplimiento del SGSI frente a los requisitos de la Norma
- Entrega formal del Manual de Seguridad de la Información
- Entrega de los Indicadores
- Entrega de la Declaración de Aplicabilidad

ESPERANZA CHARRY QUINTERO
JEFE OFICINA ASESORA DE GESTIÓN DEL RIESGO

Proyectó y Elaboró:
Mayra Montenegro
Profesional Especializado 1 OAGRI