Bogotá, 15 de octubre de 2014

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO –SARO-

INFORME III 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 S.F.C adoptó un Sistema de Administración de Riesgo Operativo -SARO-, el cual debe ser desarrollado, establecido, implementado y actualizado.

Durante el III 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 revisaron la matriz de riesgos, validando la calificación de criticidad de cada uno de los riesgos e implementando planes de tratamiento para los riesgos calificados en un nivel moderado, alto y extremo.

La Entidad registra un total de 82 Riesgos Operativos identificados para cada uno de los procesos, así:

RO	RIESGO OPERACIONAL	RO	RIESGO OPERACIONAL
1	Errores o inconsistencias en la información de la cuenta individual y la hoja de vida del afiliado	21	Falsificación documental y/o suplantación de identidad
2	Fallas en la liquidación de intereses de la cuenta del afiliado	22	Inconsistencias y/o inoportunidad en la respuesta a la solicitud realizada por el consumidor financiero
3	Errores y/o demoras en la devolución de aportes/cesantías	23	Problemas con los proyectos inmobiliarios promocionados
4	Apropiación indebida de recursos	24	Fallas en la gestión de solución de vivienda para el Fondo de Solidaridad
5	Fallas en los sistemas de información	25	Fallas o debilidades en la administración del encargo fiduciario del Fondo de Solidaridad
6	Deficiencias en el trámite de embargos y desembargos	26	Inconsistencias en el contenido de las comunicaciones externas
7	Errores en las novedades a reportar a las unidades ejecutoras	27	Apropiación ilícita de recursos del Fondo de Solidaridad
8	Errores en la elaboración de la planilla de pago del subsidio	28	Negligencia en el reporte y documentación de los riesgos
9	Demoras en el trámite de solicitud del subsidio	29	Fallas en la administración del Plan de Continuidad del Negocio -PCN-
10	Incumplimiento de la normatividad	30	Concentración de funciones
11	Incumplimiento y/o inconsistencias en la entrega de información a Entes de Control	31	Pérdida de talento
12	Inconsistencias en reportes entregados a la Alta Gerencia	32	Incumplimiento en la generación y envío de informes a autoridades administrativas y de gobierno
13	Fallas en la ejecución de la orden de negociación	33	Deficiencias en la elaboración y validación de la planificación de la gestión estratégica de la Entidad
14	Errores o inconsistencias en la valoración del portafolio de inversiones	34	Deficiencias en el cumplimiento al plan institucional por proceso y mejoramiento de la entidad
15	Fallas en el registro de inversiones	35	Deficiencia en la calidad y oportunidad en la entrega de la información requerida.
16	Atención; orientación y/o asesoría inadecuada	36	Debilidades en las competencias requeridas por el equipo auditor
17	Fallas en la gestión del trámite	37	Fallas y/o demoras en la generación de la certificación de cumplimiento para pago a contratistas
18	Inconsistencias en la base de datos de afiliados	38	Contratación de un bien o servicio que no cumpla con los términos de referencia
19	Extravío y/o deterioro de la documentación	39	Fallas o demoras en la elaboración del Plan de Contratación
20	Incumplimiento del outsourcing	40	Demoras o fallas en la representación judicial y extrajudicial de la Entidad

RO	RIESGO OPERACIONAL	RO	RIESGO OPERACIONAL
41	Errores en la emisión de conceptos jurídicos	62	Interrupción parcial o total de los servicios ofrecidos por TI
42	Fallas en la actualización de la normatividad aplicable a CAPROVIMPO en los sistemas de información	63	Fallas en el plan de recuperación de desastres -D.R.P
43	Error o demoras en el ingreso, salida y distribución de la documentación y comunicaciones de la entidad	64	Ausencia total y/o parcial de contratos de soporte y mantenimiento de los servicios de TI
44	Error o demoras en la salida de documentación y comunicaciones de la Entidad	65	Utilización indebida de información confidencial
45	Integridad y confiabilidad de la digitalización del archivo	66	Falta de personal
46	Fallas en la vinculación del personal	67	Procedimientos no documentados y/o desactualizados
47	Errores en la liquidación de nómina	68	Insuficiencia; obsolecencia y/o subutilización de los activos tecnológicos
48	Fallas en la capacitación del personal	69	Fallas de conectividad
49	Fallas en la elaboración y ejecución del Plan de Bienestar Integral	70	Interrupción en el servicio del centro de computo
50	Fallas en la desvinculación laboral	71	Fallas en la disponibilidad de los sistemas de información
51	Fallas y/o demoras en la distribución de los elementos requeridos por los procesos	72	Fallas en el respaldo y recuperación de la información
52	Fallas en la administración del inventario	73	Fallas en el seguimiento y control a contratos de tercerización
53	Fallas en la administración de la caja menor	74	Vulneración de la integridad; disponibilidad y confidencialidad de la informaciòn de la Entidad
54	Fallas en la administración de inmuebles	75	Deficiencia en la identificación del grupo objetivo
55	Errores o demoras en la consolidación y presentación del proyecto manual de presupuesto	76	Errores en la formulación de la estrategia de una camapaña de mercadeo
56	Afectación errónea de los rubros presupuestales	77	Impacto no esperado en la estrategia de la campaña
57	Errores en la elaboración de comprobantes de ingresos	78	Información deficiente o erronea al cliente interno y externo y usuarios en general
58	Demoras en el trámite de las órdenes de pago	79	Carencia o inadecuadas estrategias de educación financiera para nuestros consumidores financieros
59	Errores en la ejecución de los pagos	80	Aplicación inadecuada de la ley disciplinaria
60	Fallas y/o extemporaneidad en la liquidación; presentación y pago de obligaciones tributarias	81	Prescripción de la acción disciplinaria
61	Incumplimiento Acuerdo de Niveles de Servicio y/o Contratos de mantenimiento/soporte	82	Demora en el cumplimiento de términos en las etapas procesales

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

		Riesgo Residual Actual	
Riesgos Operativos identificados	82	Riesgo Operativo Extremo	0
		Riesgos Operativo Alto	6
		Riesgo Operativo Moderado	59
		Riesgo Operativo Bajo	17

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 bajo con una calificación de 8.34.

Para el reporte de eventos de riesgos operativo, se implementó el formato de GR-NA-FM-015 "Reporte de Eventos de Riesgo Operativo", donde los Líderes de los Procesos durante los meses de agosto y septiembre reportaron dichos REROS, dando cumplimiento con lo dispuesto en el Manual SARO y el literal a) del Numeral 3.2.5.1 Características mínimas del registro de eventos de riesgo operativo del Capítulo XXIII de la C.E. 100 de 1995.

Se revisó, analizó y actualizó cada una de las matrices de riesgos de los procesos, ajustando las causales y controles identificados para la mitigación de los riesgos. Los procesos de Gestión de Finanzas y Gestión Disciplinaria cambiaron la descripción de algunos de sus riesgos contemplados en las matrices acorde con el desarrollo de sus actividades.

En las mesas de trabajo se estableció con cada uno de los Líderes de los Procesos la elaboración de planes de tratamiento para los riesgos calificados en moderado, alto y extremo. Se creó el formato GR-NA-FM-016 "Formato Plan de Tratamiento de los Riesgos", por medio del cual fueron reportados a la Oficina Asesora de Gestión del Riesgo los tratamientos formulados por cada proceso y posteriormente se registraron en el Sistema de información Vigía - Riesgos.

APROBACIÓN DEL MANUAL SARO

En sesión extraordinaria del Comité de Riesgos realizado el 11 de septiembre/14 se aprobó la presentación del Manual SARO a la Junta Directiva.

En sesión de Junta Directiva del 17 de septiembre/14 la Oficina Asesora de Gestión del Riesgo, presentó los manuales de SAR ajustados a la propuesta del producto Leasing Habitacional donde se da viabilidad para someterlos a aprobación de la Superintendencia Financiera de Colombia, siendo radicados en dicha Entidad el 29 de septiembre/14.

REGISTRO DE EVENTOS DE RIESGO OPERATIVO - RERO

Durante el periodo comprendido entre julio y septiembre del 2014, se realizó 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 **108 REROS**, los cuales de acuerdo con lo establecido por la S.F.C. están clasificados como sigue:

Clasificación	Eventos con pérdida	Eventos sin pérdida	Total Eventos
Ejecución y administración de procesos	1	99	100
Fallas tecnológicas	0	7	7
Relaciones laborales	0	1	**1**
TOTAL	**1**	**107**	**108**

El evento de pérdida fue dictado en la resolución 320 de 2014, por valor de $1.636.062.50 por cesantías no retenidas del señor Afiliado Marco Santana identificado con C.C. 80.742.253 por orden del Juzgado Promiscuo Municipal Carmen Carupa- Cundinamarca correspondiente al proceso incidente 2003-00041 en la cuenta de Depósitos Judiciales (251542042001 con radicado 20140095474) a nombre de la Sra. María Consuelo Espitia con C.C. 20.445.117.

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 y el proceso Mercadeo y Comunicaciones reportaron **98** registros de PNC durante el tercer trimestre del 2014, distribuidos como sigue:

Proceso	Producto No Conforme
Gestión del SAC	14
Administración de Cuentas Individuales y Cesantías	14
Identificación, Afiliación y Gestión del Trámite	69
Mercadeo y Comunicaciones	1
Total	**98**

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.

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 período de reporte, brindó inducción a 29 funcionarios que ingresaron a la Entidad y capacitación a 18 funcionarios de los diferentes procesos tal como se muestra a continuación:

Mes	Funcionarios Inducción	Funcionarios Capacitados	Calificación Promedio
Julio	1	0	99.83
Agosto	13	18	96.35
Septiembre	15	0	100.00
TOTAL	**29**	**18**	**98.72**

En la inducción la Oficina Asesora de Gestión del Riesgo-OAGRI, efectuó una descripción general del Sistema de Administración de Riesgo Operativo, enfatizando en la responsabilidad que los funcionarios adquieren al ingresar a la Entidad con relación a los eventos de riesgo operativo que se puedan materializar en su proceso.

Se realizó permanente acompañamiento a los procesos en el ajuste a las matrices de riesgos en cuanto a causales y controles implementados para mitigar la materialización de los riesgos, posteriormente, se socializó la matriz de riesgo con los funcionarios de todos los procesos.

PLAN DE CONTINUIDAD DEL NEGOCIO

De conformidad con el informe reportado por el Oficial de Seguridad de la Información; durante el III 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.

a. 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 septiembre a las cámaras ip, continúan deshabilitadas, ya que al realizar el backup este consumía bastante ancho de banda.
- El DVR continúa sin funcionamiento, dado que semanas atrás este se quemó y quedando inservible, ocasionando que las cámaras quedarán 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 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, en correcto funcionamiento.
- 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.
- 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).

b. 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 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.

SEGURIDAD DE LA INFORMACIÓN

El Grupo de Seguridad de la Información realizó 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. A fin de prevenir posibles eventos de fuga de información, eventos de denegación de servicios, así como monitorear el tráfico autorizado en servicios como FTP, Telnet, SNMP, SSL, SMTP, HTTP, "correo", entre otros.

Durante el III Trimestre de 2014, en el caso del correo electrónico, se evidenció un total de 1.607.925 correos distribuidos de la siguiente manera:

CUENTAS CORREO	NUMERO DE CORREOS
cuenta caprovimpo.gov.co	1.428.420
cuenta gmail.com	10.017
cuenta hotmail.com	12.216
otros corporativos	157.272

El Grupo de Seguridad de la Información de la Oficina Asesora de Gestión del Riesgo, revisó 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 adoptaron 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 efectuó el análisis de log's de auditoría de la herramienta Solo Audi al sistema de información GA2, detectando los siguientes movimientos:

- No se crearon usuarios con privilegios, igualmente para su mejor supervisión todos los soportes se encuentran en el sistema (GA2).

- Se tomaron registros aleatorios para este informe en el período de análisis sin encontrar ninguna operación no soportada.

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

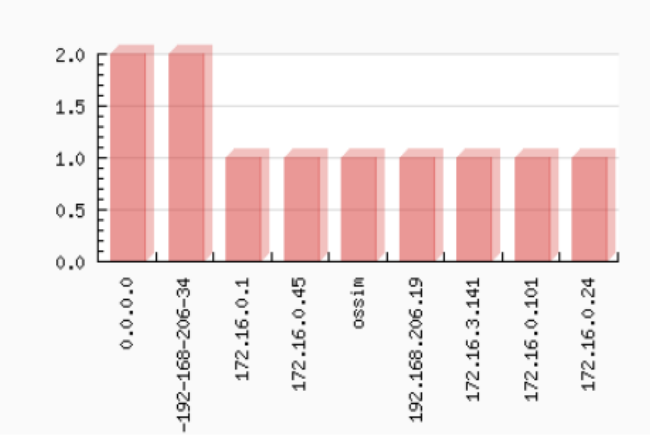
Sistema de SOC (Security Operation Center)

El Estudio de Log's 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, esta herramienta 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).

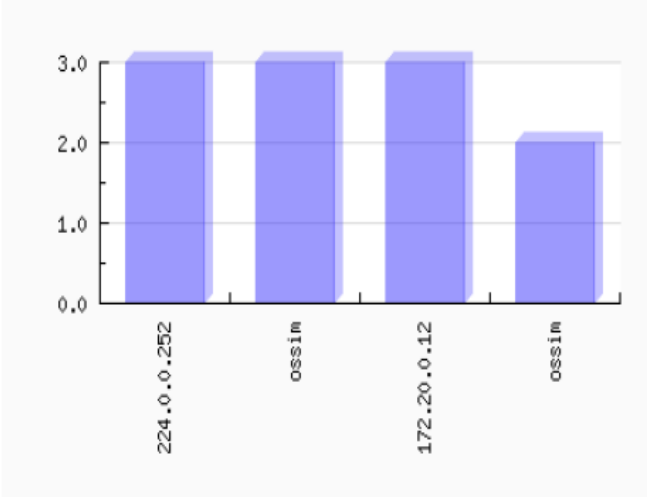
La siguiente gráfica evidencia que durante el III trimestre 2014 toda amenaza fue detectada por el Grupo de Seguridad de la Información y controlada sin generar riesgos que pudieran afectar la infraestructura tecnológica de la Entidad. Asimismo, se efectuó un completo y permanente análisis de tráfico, que salvo ataques planificados, especializados, elaborados y ejecutados por el mismo Grupo no presentaron alteraciones.

Adicionalmente, el Grupo de Seguridad de la Información monitoreó 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
0.0.0.0	2
Host-192-168-206-34	2
172.16.0.1	1
172.16.0.45	1
ossim	1
192.168.206.19	1
172.16.3.141	1
172.16.0.101	1
172.16.0.24	1

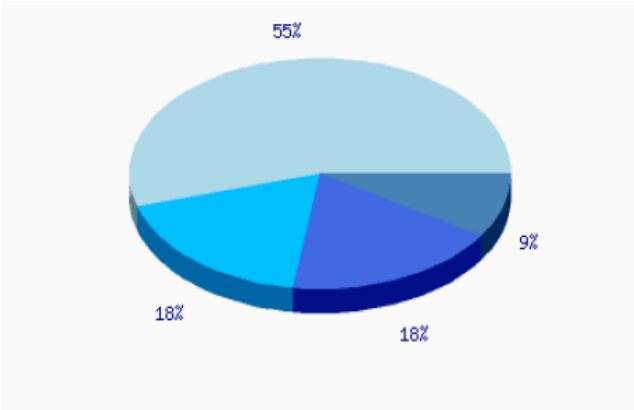


Host	Occurrences
224.0.0.252	3
ossim	3
172.20.0.12	3
ossim	2



La anterior gráfica hace referencia a potenciales ataques que pudieran haber sido generados desde o hacia nuestra red durante el último trimestre. El host 224.0.0.252 corresponde al borde de la subnet (Equipo de CAPROVMPO que detecta elementos sospechosos) es normal que generé este tráfico por su función, el 172.20.0.12 pertenece al servidor OSSIM (Herramienta SOC de La Firma Wexler S.A.A para CAPROVIMPO) el cual monitorea y verifica actividades de la red. Los demás equipos han sido hosts que se han visto afectados por spyware o malware pero que han sido corregidos y limpiados por los sistemas de limpieza de la Entidad.

Alarm	Occurrences
Environmental Awareness — Desktop Software - P2P — eDonkey	6
SSHd: Failed password	2
userdel: Check pass	2
SSHd: Invalid user	1



Alarm	Risk
SSHd: Failed password	1
SSHd: Invalid user	1
userdel: Check pass	1
Environmental Awareness — Desktop Software - P2P — eDonkey	1

En las gráficas anteriores se observan las posibles violaciones a nuestras políticas de seguridad, todas detectadas por el Grupo de Seguridad de la Información de manera controlada. No existió para el trimestre ningún ataque efectivo a nuestra plataforma.

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

Se evidenció un aumento en las vulnerabilidades altas por los nuevos sistemas de codificación de malware diseñados por el Grupo de Seguridad de la Información, por medio de pruebas realizadas en la OAGRI, se logró crear elementos maliciosos y ejecutar pruebas de concepto controladas en equipos de la Entidad, tomados al azar. Al lograr implantar este software en equipos fue posible acceder al sistema a nivel de «System» (El más alto privilegio en el sistema), también generando el respectivo informe con las recomendaciones de acción a tomar, para lo cual la Oficina Asesora de Informática -OAINF está tomando las acciones correctivas para contrarrestares estos nuevos posibles vectores de ataque.

Se recomendó evaluar el sistema antivirus de la Entidad, para Wexler S.A.S fue posible crear elementos maliciosos y ejecutarlos a través de las diferentes redes internas de la Entidad sin que existiera una reacción por parte de cualquier sistema de defensa a nivel interno. La recomendación se extiende para que a la luz de futuras adquisiciones se analice un sistema de LISTAS BLANCAS y no las listas negras actuales como se manejan todos los antivirus.

Seguimiento al cumplimiento de la Circular Externa 042 de 2012 de la S.F.C

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 TELECO	90%
3.1 SEGURIDAD Y CALIDAD	99%
3.2 TERCERIZACIÓN Y OUTSORCING	100%
3.3 DOCUMENTACIÓN	100%
3.4 DIVULGACIÓN DE INFORMACIÓN	100%
4.1 OFICINAS	94%
4.7 CENTRO DE ATENCIÓN TELEFÓNICA	100%
5. REGLAS SOBRE ACTUALIZACIÓN DE SOFTWARE	100%
7. ANÁLISIS DE VULNERABILIDADES	100%

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.

En cuanto al tema de Obligaciones Adicionales por tipo de canal (4.1 Oficinas), 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 solo se cuenta con CCTV para la sede Bogotá- CAN).

Con respecto al tema de Obligaciones Generales, en el numeral 3.1.20 no todas las oficinas 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 el mes de julio, agosto y septiembre, para un total de 44 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 Inducción	Funcionarios Capacitados	Calificación Promedio
Julio	1	0	100.00
Agosto	13	0	92.31
Septiembre	15	15	92.00
TOTAL	**29**	**15**	**94.77**

Acompañamientos especiales y proyectos específicos

Acompañamiento PCN

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

Se efectuó la programación, preparación, diseño y ejecución de las pruebas técnicas de continuidad de operaciones comprobando la operatividad de la Entidad desde el centro alterno de datos (Ortezal); validando que los datos contenidos en las Bases de Datos y las aplicaciones funcionaron correctamente para: INTRANET, SAC, GA2, *FOLIUM, *PORTAL, KACTUS, SEVEN, VIGIA M&C, DIALOGO, VIGIA RIESGOS, BISTALK, ORION JURIDICO y ORION DISIPLINARIO.

*(Las pruebas para estos sistemas se efectuaron dos días después de los otros sistemas por limitaciones técnicas que fueron resueltas en el transcurso de ese tiempo).

Asimismo, se efectuó la programación, preparación diseño y ejecución de un simulacro de continuidad de operaciones comprobando la operatividad de la Entidad desde el centro alterno de datos (Ortezal), validando fue posible efectuar un proceso completo desde la llegada del Afiliado hasta la generación del pago, los sistemas que intervinieron y se verificaron en continuidad para esta operación fueron: INTRANET, SAC, GA2, FOLIUM, PORTAL, KACTUS, SEVEN, VIGIA M&C, DIALOGO, VIGIA RIESGOS, BISTALK, ORION JURIDICO y ORION DISIPLINARIO. Los resultados de la prueba permitieron validar que es posible la ejecución de trámites desde nuestro centro alterno de datos en continuidad.

Portal Transaccional

Se efectuaron hasta el momento del cierre del tercer trimestre de 2014, 2 análisis de vulnerabilidades sobre el portal transaccional generando las recomendaciones respectivas.

Validación de licenciamiento

Se llevó a cabo un análisis y una auditoría tomando como muestra el 10% de las máquinas de la Entidad tanto en la sede principal como en cada uno de los puntos de atención, validando que todo software instalado este autorizado y debidamente licenciado para la muestra analizada.

CAPROVIMPO durante el trimestre contó con una disponibilidad de la plataforma informática superior al **97%** y 0 ataques efectivos a la plataforma, disponibilidad de Correo 97.0%, Directorio Activo 97.2%, Plataforma GA2 97.1%, Plataforma DIALOGO 96.3%, Plataforma FOLIUM 95.97%, Intranet 97.9%.

El **3%** consolidado de no disponibilidad de la plataforma obedeció a preparación y ejecución de las pruebas de continuidad de operación y simulacros de continuidad programadas por la Entidad en tiempos no laborales y fines de semana, en días ordinarios después de las 8 p.m.

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 Informática.

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.

Se llevó a cabo una auditoría de prueba con el fin de validar este nivel de cumplimiento generando la respectiva matriz de control y remediación, a la cual se le efectuó el correspondiente seguimiento.

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	Pérdida 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

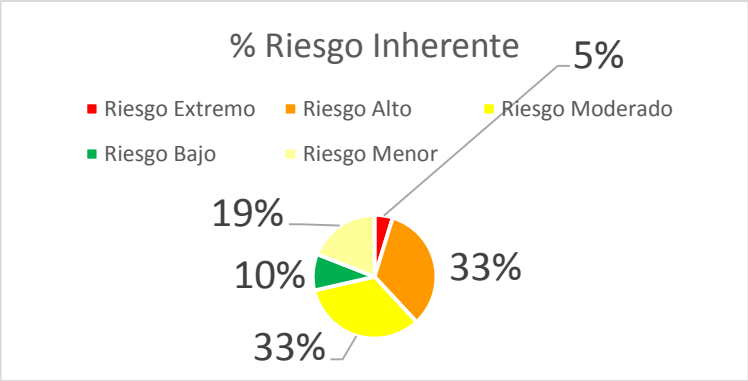
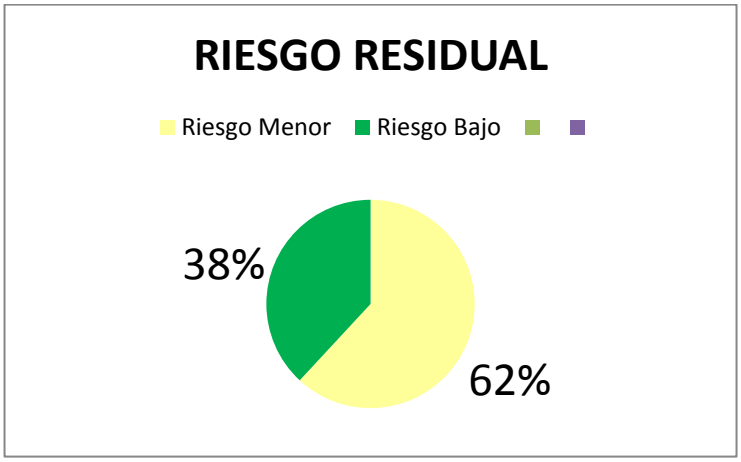


Figura 2. Riesgos Residuales



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.

- 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.

- Culturización

Como parte de la necesidad y requisito indispensable de establecer el SGSI en CARPOVIMPO, 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.

- 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 a la OAGRI.

•Entrega de los Indicadores

•Entrega de la Declaración de Aplicabilidad

LINA MARIA RENDON LOZANO
JEFE OFICINA ASESORA DE PLANEACION ENCARGADA
DE LAS FUNCIONES DE JEFE DE OFICINA ASESORA DE GESTIÓN DEL RIESGO

Elaboró:
Fanny Rodríguez Cuervo
Profesional Universitario 3 OAGRI