Bogotá, 15 de enero de 2015

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO –SARO-
INFORME IV TRIMESTRE DE 2014

La Caja Promotora de Vivienda Militar y de Policía 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 IV trimestre de 2014 se realizó revisión de los riesgos operativos a través de un trabajo de campo al proceso misional de la Entidad "Administración de Cuentas Individuales y Cesantías", donde se identificaron los posibles riesgos en la ejecución de cada uno de los procedimientos con la finalidad de que los Líderes implementen nuevos controles y planes de acción para mitigarlos.

La OAGRI, realizó monitoreo a los Planes de Tratamiento de once (11) proceso; implementados para los riesgos residuales extremos, altos y moderados, para lo cual dicha implementación ha sido efectiva de acuerdo con lo reportado por los líderes de los procesos.

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:

CONCEPTO	CANTIDAD	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 sobre 20.

REGISTRO DE EVENTOS DE RIESGO OPERATIVO - RERO

Durante el periodo comprendido entre octubre a diciembre 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 **179 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	169	170
Fallas tecnológicas	0	6	6
Eventos Externos	0	2	2
Relaciones laborales	0	1	1
TOTAL	**1**	**178**	**179**

El evento de pérdida fue dictado en la resolución 621 de 2014, por valor de $4.486.480, por Autoprobatorio de Conciliación Prejudicial del 24 de noviembre/14 celebrada ante Procuraduría 58 de Asuntos Administrativos en la ciudad de Cali correspondiente al proceso judicial 76001-33-33-012-2014 del señor Afiliado Elicer Yepes identificado C.C. 80.795.281 (valor que le fue descontado de las cesantías), girado el 23 de diciembre/14 a favor del señor apoderado José Manuel Cáceres Martínez con C.C. 16.479.637.

De acuerdo con el análisis efectuado a los riesgos operativos reportados, se realizó acompañamiento a los procesos y en especial a los Líderes del proceso de Administración de Cuentas Individuales y Cesantías en cuanto a causales y controles implementados para mitigar la materialización de los riesgos operativos, realizando mesas trabajo y solicitando los controles respectivos.

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 **157** registros de PNC durante el cuarto trimestre del 2014, distribuidos como sigue:

Proceso	Producto No Conforme
Identificación, Afiliación y Gestión del Trámite	76
Administración de Cuentas Individuales y Cesantías	67
Gestión del SAC	14
Total	**157**

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 **18** funcionarios que ingresaron a la Entidad de los diferentes procesos tal como se muestra a continuación:

Mes	Funcionarios Inducción	Calificación Promedio
Noviembre	18	98.75

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.

PLAN DE CONTINUIDAD DEL NEGOCIO

De conformidad con el informe reportado por el Oficial de Seguridad de la Información; durante el IV 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 diciembre 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.
- Se observa que los extintores se encuentran con fecha de recarga actualizada (Diciembre 2014). De acuerdo a esto es necesario que se efectué la recarga de manera inmediata antes del 31 de diciembre de 2014.
- Racks de comunicación de voz y datos: 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. 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 IV Trimestre de 2014, en el caso del correo electrónico, se evidenció un total de 325.467 (se nota una disminución en el número de coreos debido al boqueo de las cuantas de correos no corporativos solicitada por el grupo de seguridad de la información de la Oficina Asesora de Gestión de Riesgo y ejecutado por la Oficina Asesora de Gestión Informática // y el periodo de licencia) de correos distribuidos de la siguiente manera:

CUENTAS CORREO	NUMERO DE CORREOS
cuenta caprovimpo.gov.co	290.257
cuenta gmail.com	4.139
cuenta hotmail.com	5.598
otros corporativos	25.473

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.

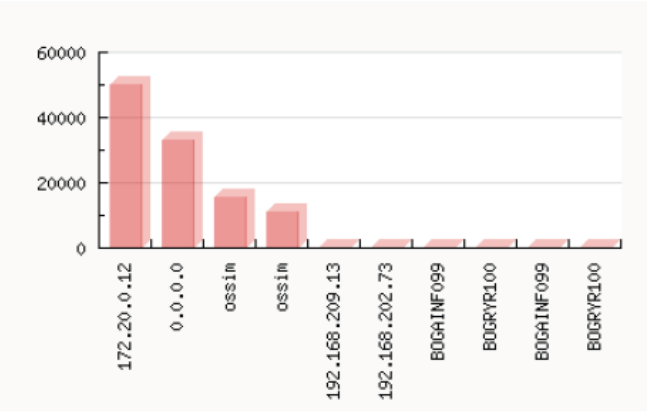
Sistema de SOC (Security Operation Center)

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).

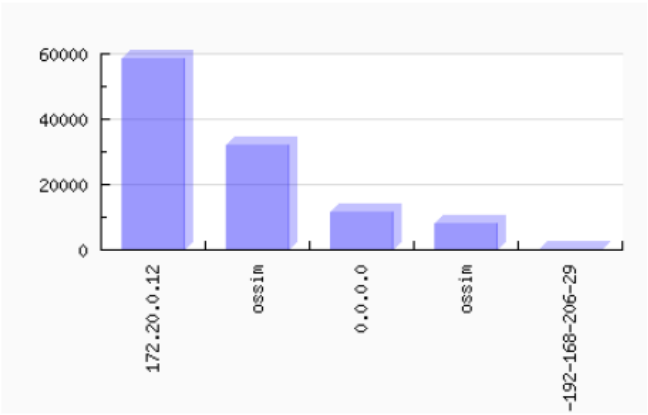
La siguiente gráfica evidencia que durante el IV trimestre 2014 toda amenaza fue detectada por el Grupo de Seguridad de la Información y controlada sin generar riesgos que pudieran afectar la infraestructura tecnológica de la Entidad. Asimismo, se efectuó un completo y permanente análisis de tráfico, 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.

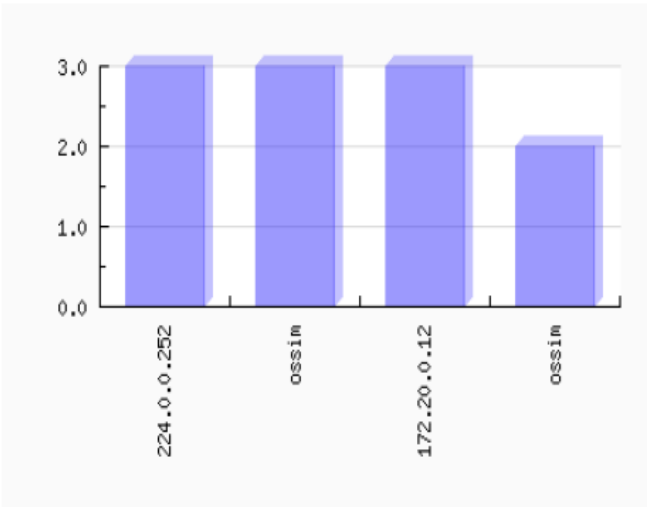
Host	Occurrences
172.20.0.12	50.155
0.0.0.0	33.134
ossim	15.527
ossim	11.131
192.168.209.13	68
192.168.202.73	37
BOGAINF099	23
BOGRYR100	18
BOGAINF099	18
BOGRYR100	13



Host	Occurrences
172.20.0.12	58.487
ossim	32.095
0.0.0.0	11.743
ossim	7.823
Host-192-168-206-29	1

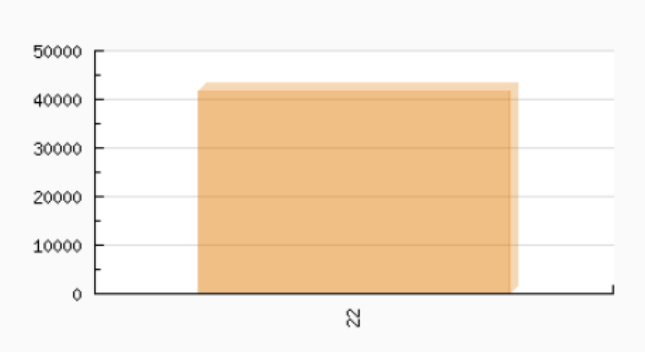


Host	Occurrences
224.0.0.252	3
ossim	3
172.20.0.12	3
ossim	2

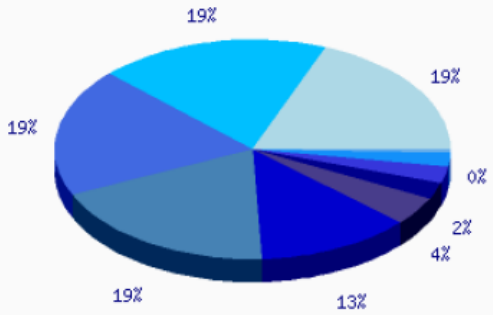


La anterior gráfica hace referencia a potenciales ataques que pudieran haber sido generados desde o hacia nuestra red durante el último trimestre. El host 224.0.0.252 corresponde al borde de la subnet (Equipo de la Entidad que detecta elementos sospechosos) es normal que generé este tráfico por su función, 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.

Port	Service	Occurrences
22	ssh	41.611



Event	Occurrences
ossec: SSHD authentication success.	20.807
ossec: Login session closed.	20.807
SSHd: Received disconnect	20.806
SSHd: Login sucessful, Accepted publickey	20.805
ossec: Successful login during non-business hours.	13.899
ossec: Login session opened.	4.677
sudo: Command executed	2.676
ossec: Successful sudo to ROOT executed	2.661
ossec: Successful login during weekend.	2.232
ossec: Kernel Input/Output error	536
nagios: host alert - soft down	141
nagios: service alert - soft warning	26
nagios: service alert - hard warning	17
nagios: service alert - hard ok	17
nagios: service alert - soft critical	14



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

El análisis de vulnerabilidades efectuado de menara permanente durante el último trimestre del año 2014 arrojo como resultado una permanencia de las vulnerabilidades de nivel crítico detectadas en el trimestre anterior; esto como consecuencia del proceso de estabilización que está efectuando la Oficina Asesora de Informática y a que está pendiente la culminación de la fase II del proyecto de seguridad informática que se tiene contemplado para esta culminado en Marzo de 2015.

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%

ITEM	CUMPLIMIENTO
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 noviembre, 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
Noviembre	75	75	96
TOTAL	**75**	**75**	**96**

Acompañamientos especiales y proyectos específicos

1. Portal Transaccional

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

2. 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.

La Caja Promotora de Vivienda Militar y de Policía contó con:

- Una disponibilidad de la plataforma informática superior al **98%**
- Cero (0) ataques efectivos a la plataforma
- Disponibilidad de Correo 97.0%
- Directorio Activo 98.2%,
- Plataforma GA2 98.1%,
- Plataforma DIALOGO 96.3%,

- Plataforma FOLIUM 95.97%,
- Intranet 97.9%.

El **2%** consolidado de no disponibilidad de la plataforma obedeció a preparación y ejecución mantenimientos y soportes programadas por la Entidad en tiempos no laborales y fines de semana, en días ordinarios después de las 8 p.m.

JHON JAIRO ROSAS ALBA
JEFE OFICINA ASESORA DE GESTION DEL RIESGO

Elaboró:
Fanny Rodríguez Cuervo
Profesional Universitario 3 OAGRI