ALCALDÍA MAYOR DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial Catastro Distrital

UNIDAD ADMIN. CATASTRO DISTRITAL 20-11-2017 04:29:20
Al Contestar Cite Este Nr.:2017IE15869 O 1 Fol:1 Anex:0
ORIGEN: Origen: Sd:19 - OFICINA DE CONTROL INTERNO/VILLAMIL MU
DESTINO: Destino: DIRECCION GENERAL/PUENTES RIAÑO CLAUDIA CI
ASUNTO: Asunto: INFORME DE SEGUIMIENTO AL COMITÉ DE SEGURI
OBS: Obs.: PROYECTO/ ALEXANDRA YOMAYUZA

MEMORANDO

Unidad Administrativa Especial de Catastro Distrital
DIRECCIÓN
21 NOV 2017
RECIBIDO
HORA: 11:43 T.L.

Referencia: Plan Operativo Anual de la Oficina de Control Interno Vigencia 2017

Fecha : 20 de noviembre de 2017

PARA : Claudia Puentes Riaño
Directora UAECD

DE : Alba Enidia Villamil Muñoz
Jefe Oficina de Control Interno

ASUNTO : Informe de seguimiento al Comité de Seguridad de la Información y Continuidad de Negocio

En desarrollo del Plan Operativo Anual de la Oficina de Control Interno establecido para la vigencia 2017, la Oficina de Control Interno realizó seguimiento al Comité de Seguridad de la Información y Continuidad de Negocio, cuyos resultados se presentan a continuación.

1. OBJETIVO

Realizar seguimiento al Comité de Seguridad de la Información y Continuidad de Negocio.

2. ALCANCE

Funciones desarrolladas por el Comité de Seguridad de la Información y Continuidad de Negocio entre el 1 de junio de 2017 y el 31 de octubre de 2017.

3. MARCO NORMATIVO

Resolución 2806 de 2015 "Por la cual se unifican las reglas de creación del Comité de Seguridad de la información y continuidad de negocio de la UAECD y se derogan las Resoluciones No. 167 de 2010, 1094 de 2011, 0318 de 2013 y 1514 de 2014".

4. METODOLOGÍA

El seguimiento se realizó dentro del marco de las normas de auditoría generalmente aceptadas, e incluyó: la planeación, el análisis de la normatividad vigente, los procedimientos y demás documentación asociada; la verificación de la información suministrada y la elaboración del informe con las conclusiones y recomendaciones que permitan mejorar el sistema de control interno.

5. PRESENTACIÓN DE RESULTADOS

5.1 Verificación de la realización de las reuniones del Comité de Seguridad de la Información y Continuidad de Negocio de acuerdo con lo dispuesto en los artículos 4 y 5 de la Resolución 2806 de 2015.

Según la Resolución 2806 de 2016, artículo 4 *"El Comité de Seguridad de la Información y Continuidad de Negocio será conformado por los siguientes servidores públicos, quienes concurrirán como miembros permanentes, con voz y voto:*

1. *El Director*
2. *El Gerente de Tecnología*
3. *El Gerente de Información Catastral*
4. *El Gerente de Gestión Corporativa*
5. *El Gerente de Infraestructura de Datos Espaciales (IDECA)*
6. *El Gerente Comercial y de Atención al Usuario*
7. *El Jefe de la Oficina Asesora de Planeación y Aseguramiento de Procesos*
8. *El Oficial de Seguridad de la Información, adscrito a la Gerencia de Tecnología*
9. *El Oficial de Continuidad de Negocio, adscrito a la Gerencia de Tecnología*

(...)"

El artículo 5 dispone respecto a las reuniones, el quórum deliberativo y toma de decisiones:

"El Comité de Seguridad de la Información y de Continuidad de Negocio de la Entidad sesionará en forma ordinaria al menos una (1) vez cada semestre y en forma extraordinaria cuando sea necesario por solicitud de cualquiera de sus miembros.
Para tales efectos sesionará como mínimo, con la mitad más uno de sus miembros, señalados por el Artículo 4 del presente instrumento, y adoptará las decisiones por mayoría simple. Lo anterior aplica tanto para las sesiones presenciales como las virtuales.
(...)"

Situaciones evidenciadas

Se observó que se programaron y realizaron cinco sesiones del Comité de Seguridad de la Información y Continuidad de Negocio en el período evaluado, alcanzando un total de seis sesiones en la vigencia:

Tabla 1. Desarrollo de las sesiones del Comité de SICN

Acta	Fecha	Quórum	Temas tratados
Acta No. 2 Ordinaria	16 de junio de 2017	9 asistentes: Directora, 5 Gerentes, 2 Oficiales de cumplimiento, 1 Jefe Oficina	Se sometieron a consideración del Comité y se aprobaron ocho (8) documentos del SGSI, entre los que se encuentra el Manual del SGSI , se realizó seguimiento a la auditoría de control interno, así como al hallazgo de la auditoría de la Contraloría, seguimiento al Sistema de Gestión Continuidad de negocio y al Sistema de Gestión Seguridad de la Información; se presentan los avances en el concurso "Máxima Velocidad", disposiciones respecto a medios removibles y difusión de instrumentos de gestión de activos en el marco del SGSI; se realizó seguimiento a los compromisos de comités anteriores.
Acta No. 3 Ordinaria	24 de agosto de 2017	8 asistentes: Directora, 4 Gerentes, 2 Oficiales de cumplimiento, 1 Jefe Oficina	Se realizó sensibilización a nivel ejecutivo y táctico. Se presentó el estado de la contratación asociada a SGSI. Continuidad de negocio: Seguimiento al plan de trabajo, estado del indicador de oportunidad en

Acta	Fecha	Quórum	Temas tratados
			cumplimiento del RTO, árbol de llamadas para el manejo de crisis. Seguridad de la información: Seguimiento al plan de trabajo, avances en la ejecución del plan de capacitación, sensibilización y comunicación, estado de los incidentes de seguridad de la información, propuesta para medir el indicador de apropiación de instrumentos de SI, plan de trabajo de documentación, acompañamiento solicitado a MinTIC para transición a IPv6, resultados del seguimiento de la OCI al cumplimiento de las funciones del Comité, hallazgo de la Contraloría respecto al contrato 056-2015. Se le comunicó al Comité el resultado de la evaluación del nivel de seguridad tecnológica de la Unidad. Se presentaron los avances en el concurso Máxima Velocidad.
Acta No. 4 Extraordinaria	14 de septiembre de 2017	9 asistentes: Directora, 5 Gerentes, 2 Oficiales de cumplimiento, 1 Jefe Oficina	Modificación de la fecha para realizar pruebas funcionales del DRP
Acta No. 5 Ordinaria	5 de octubre de 2017	7 asistentes: 4 Gerentes, 2 Oficiales de cumplimiento, 1 Jefe Oficina	Estado de la documentación de Seguridad de la Información, Recomendaciones para prevenir ataque DDOS, uso de medios removibles, Continuidad de Negocio: árbol de llamadas, Boletines de seguridad publicados, resultados concurso máxima velocidad, estado de la contratación de la consultoría.
Pendiente acta Ordinaria	26 de octubre de 2017	7 asistentes: 4 Gerentes, 2 Oficiales de cumplimiento, 1 Jefe Oficina	Continuidad de negocio: plan de manejo de crisis, Presentación COLCERT incidentes de ciberseguridad

Fuente: Actas suministradas por la Secretaria Técnica del Comité

Se evidenció que todas las reuniones fueron convocadas por la Secretaria Técnica del Comité. Se convocó a la Directora de la UAECD, Gerente de Información Catastral, Gerente Comercial y de Atención al Usuario, Gerente de Gestión Corporativa, Gerente Ideca, Gerente de Tecnología, Jefe Oficina Asesora de Planeación y Aseguramiento de Procesos, Oficial de Seguridad de la Información, Oficial de Continuidad de Negocio y se convocó como invitados a la Jefe de la Oficina de Control Internoy al Jefe Oficina Asesora Jurídica.

Se observó que en todas las reuniones se conformó quórum decisorio, cumpliendo con lo dispuesto en los artículos 4 y 5 de la Resolución 2806 de 2015.

5.2 Verificación de la realización de las funciones asignadas al Comité de SICN

El artículo 3° de la Resolución 2806 de 2015 define las siguientes funciones del Comité de Seguridad de la Información y continuidad de negocio:

"*1. Evaluar y aprobar las estrategias de seguridad de la información y continuidad de negocio.*
2. *Aprobar la política, los objetivos, el alcance y la declaración de aplicabilidad del Subsistema de Gestión de Seguridad de la Información y la política, los objetivos, el alcance del Subsistema de Gestión de Continuidad de Negocio que requiera la Entidad, de acuerdo con su contexto organizacional, proponer ajustes cuando lo considere pertinente y garantizar que sean comunicados a la UAECD.*
3. *Fijar directrices institucionales para la aplicación de mecanismos de protección de la información y la continuidad de negocio.*
4. *Asegurar que los roles y responsabilidades pertenecientes a la seguridad de la información y continuidad de negocio se asignen y comuniquen.*
5. *Facilitar la consecución y asignación de recursos que garanticen la implementación de las estrategias de continuidad de negocio y de seguridad de la información.*
6. *Aprobar y adoptar "Planes de continuidad y recuperación de Desastres" que garanticen la continuidad de las operaciones ante una situación crítica que pueda amenazar, parcial o totalmente, la prestación de servicios, planes que deberán: (i) ser avalados por la Alta Dirección; (ii) ser socializados en todos los niveles de la UAECD en el sentido de establecer las funciones y responsabilidades correspondientes, y (iii) ser revisados en caso de ser requerido, de acuerdo con el "Plan Estratégico de Tecnologías de la Información y Comunicaciones" y con cambios en las condiciones operativas de la Entidad.*
7. *Aprobar las actualizaciones que deban realizarse al Subsistema de Gestión de Seguridad de la Información y al Subsistema de Gestión de la Continuidad de Negocio en virtud de los cambios organizacionales, tecnológicos o del entorno de la operación de la Entidad.*
8. *Aprobar y hacer seguimiento a los programas periódicos de ejercicios y pruebas de la infraestructura tecnológica y continuidad de negocio, para asegurar su disponibilidad y funcionalidad permanentes.*
9. *Revisar el desempeño del Subsistema de Gestión de Seguridad de la Información y del Subsistema de Gestión de Continuidad de Negocio para asegurar su conveniencia, adecuación y eficacia continuas.*
10. *Revisar y hacer seguimiento a los requerimientos de entes externos en lo referente a la seguridad de la información y la continuidad de negocio de la Entidad.*
11. *Evaluar y analizar los incidentes de seguridad de la información cuyo impacto sea relevante para la Entidad (el nivel de relevancia lo establece el Oficial de Seguridad de la Información).*
12. *Promover el desarrollo de programas de sensibilización y concientización, capacitación y entrenamiento de los servidores públicos en seguridad de la información.*
13. *Buscar la integración de los requisitos del Subsistema de Gestión de Seguridad de la Información, cuyo marco normativo es la norma ISO27001, en los procesos de la Entidad y su articulación frente a los requisitos aplicables para el SGI establecidos en la Norma Técnica Distrital NTD SIG 001:2011 o aquella que la modifique o sustituya y demás disposiciones legales que apliquen."*

Situación evidenciada

Se evidenció de acuerdo con las actas y presentaciones al Comité, que en el período analizado se cumplieron las siguientes funciones por parte del Comité:

MEMORANDO

Función 1. Se aprobó por parte del Comité la estrategia para la prevención de ataques de DDoSel bloqueo de peticiones recibidas desde direcciones IP provenientes deRusia, China y Corea del Sur (Acta 5 de 2017 2.2 b.)

Función 2. Se realizó seguimiento por parte del Comité a los boletines de seguridad de la información (Acta 5 de 2017 2.4a.).

Función 3. Se aprobó por parte del Comité los ajustes al Manual del SGSI, la estrategia de planificación y control operacional del subsistema de gestión de seguridad de la información, así como la actualización de los procedimientos de Gestión de Incidentes de SI, Gestión de activos en el marco del SI, Gestión de riesgos sobre activos en el marco de SI, Planificación y Control de Continuidad de Negocio, Análisis de impacto al negocio y análisis de riesgos, Estrategia de Continuidad de Negocio, Implantación de planes de Continuidad de Negocio, Ejercicios y Pruebas (Actas 2, 3 y 5 de 2017).

Función 4. Se revisó por parte del Comité el ajuste al Manual de Funciones y se solicitó reactivar dicha solicitud para presentar a la CNSC (Acta 2 de 2017 numeral 3 Compromiso 6).

Función 5. Se presentó al Comité el seguimiento a las líneas de contratación incluidas en el plan de adquisiciones relacionadas con Seguridad de la información y Continuidad de negocio (Acta 3 de 2017 numeral 2.3).

Función 6. Se presentó al Comité el Plan de manejo de crisis,y la realización de pruebas funcionales de DRP (Acta 4 de 2017, Sesión del 26 de octubre de 2017 sin acta aún).

Función 7. Se realizó seguimiento a los planes de trabajo de los subsistemas de gestión de seguridad de la información y de continuidad de negocio. Se aprobó por parte del Comité los ajustes ala documentación de los subsistemas, derivados de los cambios identificados, tales como Manual del SGSI, la estrategia de planificación y control operacional del subsistema de gestión de seguridad de la información, procedimientos asociados a Continuidad de Negocio y procedimientos asociados a seguridad de la Información (Actas2, 3 y 5 de 2017).

Función 8. Se presentó al Comité el resultado de la evaluación del nivel de seguridad tecnológica realizado por proveedores externos (Acta 3 de 2017 numeral 2.5). Se aprobó por parte del comité la realización de pruebas funcionales del DRP (Acta 4 de 2017).

Función 9. Se realizó seguimiento al desempeño de los subsistemas, a partir del seguimiento al plan de trabajo de la vigencia y el resultado de los indicadores de gestión del proceso (Actas2 y 3 de 2017).

Función 10. Se realizó seguimiento a los requerimientos formulados y atendidos por parte de la Contraloría de Bogotá en el marco de la Auditoría regular de la vigencia 2016, así como al resultado del informe de Control Interno (Actas2 y 3 de 2017).

Función 11. Se presentó al Comité los incidentes de seguridad de la información, con indicación de número, estado, categoría, resumen, actividades realizadas, lecciones aprendidas (Actas 2 y 3 de 2017).

Función 12. Se realizó seguimiento a los avances del plan de capacitación, sensibilización y comunicación del SGSI aprobado por el Comité (Actas2 y 3 de 2017).

Función 13. La integración de los requisitos de seguridad de la información en los procesos de la entidad se encuentra establecida en el Manual del SGI, el cual fue actualizado en el aplicativo ISODOC el 28 de septiembre (Actas2, 3 y 5 de 2017).

MEMORANDO

Se observó en el seguimiento que la documentación aprobada por el Comité relacionada con el cumplimiento de las funciones 2, 4 y 7 del Comité, que se presentó baja participación por parte de los integrantes en la revisión del contenido de los documentos remitidos, razón por la cual se dejó la siguiente observación en el acta No. 2 del Comité del 16 de junio de 2017:

> "*2.2 Documentos aprobados por el Comité*
> *Durante la presente sesión se relacionan, en la Diapositiva 8 de la presentación, los documentos aprobados por el Comité desde la última sesión a la fecha y la participación en la revisión de los mismos por parte de los integrantes del mismo. Se solicita a los integrantes de este Comité una mayor participación en la revisión de los documentos que se someten a su revisión y aprobación*".

Gráfica 1. Diapositiva 8

2. DOCUMENTOS APROBADOS POR COMITÉ

Observaciones realizadas por / Documento aprobado por Comité	Directora	Gerencia Comercial y de Atención al Usuario	Gerencia de Información Catastral	Gerencia de Infraestructura de Datos Espaciales	Gerencia de Gestión Corporativa	Oficina de Planeación y Aseguramiento de Procesos	Oficina de Control Interno (invitada)	Oficina Asesora Jurídica (invitada)
Encuesta seguridad de la información							X	
Plan de trabajo SGSI - 2017								
Plan de trabajo SGCN - 2017								
Instructivo Comité		X						
Manual SGSI		X						
Acuerdos confidencialidad (3)		X						
Material Sensibilización								
Transferencia de Información		X			X		N/A	
Porcentaje participación	0%	50%	0%	0%	12.5%	0%	14%	0%

NOTA: Se excluye la Gerencia de Tecnología, el Oficial de Seguridad de la Información y el Oficial de Continuidad del negocio, quienes pertenecen a dicha Gerencia, ya que los documentos propuestos generados y presentados a nombre de la Gerencia de Tecnología.

Fuente: Presentación Comité del 16/06/2017

Se observó que persiste la falta de participación de los integrantes del Comité en la revisión de los documentos asociados al cumplimiento de dichas funciones, tal como se evidenció en los correos del 11 de septiembre de 2017 y del 15 de septiembre de 2017, en los que se indica por parte de la Secretaria Técnica del Comité que no se

recibieron observaciones sobre los documentos enviados, por tanto se consideran aprobados por parte de los integrantes del Comité de Seguridad de la Información y Continuidad de Negocio (Ver gráficas 2 y 3).

Gráfica 2. CompromisoN°1a_ComiteN°3

GT: Seguridad de la información y continuidad del negocio - Sesión Comité N°3 - documentos aprobados por parte de los integrantes del Comité (Manual SGSI actualizado, autodiagnóstico seguridad)

Tania Barrera Rodriguez <tbarrera@catastrobogota.gov.co> 11 de septiembre de 2017, 7:46
Para: Claudia Puentes Riaño <cpuentes@catastrobogota.gov.co>, Eliecer Vanegas Murcia <evanegas@catastrobogota.gov.co>, Olga Lucia Lopez Morales <ollopez@catastrobogota.gov.co>, Sandra Patricia Samacá <ssamaca@catastrobogota.gov.co>, Ligia Gonzalez <lgonzalez@catastrobogota.gov.co>, Orlando José Maya Martinez <omaya@catastrobogota.gov.co>, José Abraham Villarraga Rios <jvillarraga@catastrobogota.gov.co>, Andres Fernando Agudelo Aguilar <afagudelo@catastrobogota.gov.co>
Cc: Isis Johanna Gomez Peralta <ijgomez@catastrobogota.gov.co>

Buenos días a Todos,

De acuerdo con los compromisos establecidos en la sesión N° 3 del Comité de Seguridad de la Información y Continuidad del Negocio realizada el pasado 24 de agosto de 2017, se informa que:

1. No se recibieron observaciones al *Documento técnico manual del Subsistema de gestión de seguridad y privacidad de la información SGSI*, por lo cual el documento ManualSGSI_20170828.doc, enviado el pasado 28 de agosto de 2017, se considera aprobado por parte de los integrantes del Comité de Seguridad de la Información y Continuidad del Negocio.

2. No se recibieron observaciones al documento *Autodiagnóstico de seguridad de la información*, por lo cual el documento: AutodiagnosticoSGSI_20170828.xlsx, enviado el pasado 28 de agosto de 2017, se considera aprobado por parte de los integrantes del Comité de Seguridad de la Información y Continuidad del Negocio.

Muchas gracias por su atención.

NOTA. Recuerden que hasta mañana se estarán recibiendo observaciones al documento *Documento técnico estrategia de planificación y control operacional del subsistema de gestión de seguridad de la información.*

Muchas gracias por su atención.

Fuente: Evidencias cumplimiento de compromisos Comité No. 5 de 2017.

Gráfica 3. CompromisoN°1b_ComiteN°3

GT: Seguridad de la Información y continuidad del negocio - documento aprobado por parte de los integrantes del Comité: Documento técnico estrategia de planificación y control operacional del Subsistema de Gestión de Seguridad de la Información.

Tania Barrera Rodriguez <tbarrera@catastrobogota.gov.co> 15 de septiembre de 2017, 8:32
Para: Claudia Puentes Riaño <cpuentes@catastrobogota.gov.co>, Ligia Gonzalez <lgonzalez@catastrobogota.gov.co>, Sandra Patricia Samacá <ssamaca@catastrobogota.gov.co>, Olga Lucia Lopez Morales <ollopez@catastrobogota.gov.co>, Andres Fernando Agudelo Aguilar <afagudelo@catastrobogota.gov.co>, Orlando José Maya Martinez <omaya@catastrobogota.gov.co>, José Abraham Villarraga Rios <jvillarraga@catastrobogota.gov.co>, Eliecer Vanegas Murcia <evanegas@catastrobogota.gov.co>
Cc: Alba Enidia Villamil Muñoz <avillamil@catastrobogota.gov.co>, Cesar Norberto Albarracin Ochoa <calbarracin@catastrobogota.gov.co>, Isis Johanna Gomez Peralta <ijgomez@catastrobogota.gov.co>

Buenos días a todos,

De acuerdo con los compromisos establecidos en la sesión N° 3 del Comité de Seguridad de la Información y Continuidad del Negocio realizada el pasado 24 de agosto de 2017, se informa que:

1. No se recibieron observaciones al *Documento técnico estrategia de planificación y control operacional del Subsistema de Gestión de Seguridad de la Información*, por lo cual el documento enviado el pasado 5 de septiembre de 2017 se considera aprobado por parte de los integrantes del Comité de Seguridad de la Información y Continuidad del Negocio.

Muchas gracias por su atención

Fuente: Evidencias cumplimiento de compromisos Comité No. 5 de 2017.

Al respecto,se recomienda acoger la solicitud de la Secretaria Técnica del Comité, en cuanto a una mayor participación en la revisión de los documentos que se someten a su revisión y aprobación por parte de los integrantes del Comité. Adicionalmente, se recomienda que en las actas de Comité quede explícito que se sometió a consideración del comité las aprobaciones requeridas, así como el resultado correspondiente.

5.3 Verificación del cumplimiento de las funciones del Secretario Técnico del Comité.

El artículo 8° de la Resolución 2806 de 2015 dispone respecto a las funciones del Secretario Técnico del Comité:

1. *Coordinar los temas y orden del día y convocar a las reuniones del Comité. En el orden del día se deberá incluir un punto relacionado con el seguimiento a los compromisos previos relacionados con el acta del Comité anterior.*
2. *Enviar a los integrantes la información a tratar según la agenda propuesta, con una antelación no inferior a tres (3) días hábiles a la sesión.*
3. *Velar por el buen funcionamiento del Comité.*
4. *Elaborar las actas de cada sesión y enviarlas para aprobación y firma de los miembros permanentes que hayan asistido.*
5. *Verificar el cumplimiento de las decisiones adoptadas en el seno de las reuniones.*
6. *Proyectar, proponer, presentar y someter a consideración del Comité las políticas, normas, acciones o buenas prácticas necesarias para incorporar o aplicar, o ambas, en la Gestión de la Seguridad de la Información de la Entidad.*
7. *Las demás que le sean asignadas por el Comité.*

Adicionalmente, el parágrafo del artículo 6 de la Resolución 2806 de 2015 dispone que "*El Secretario Técnico designado del Comité elaborará las actas ejecutivas del desarrollo de la sesión*".

Situaciones evidenciadas

Funciones 1, 2 y 3. Se observó que la Secretaria Técnica del Comité (Oficial de Seguridad de la Información) realizó la citación a los integrantes del Comité, indicando la agenda a tratar. Se observó que en los comités realizados presentó los temas programados según la agenda propuesta.

Función 4. Se evidenció que se elaboró y se encuentran suscritas las Acta No. 2, 3, 4 y 5 de 2017, encontrándose pendiente el acta de la sesión del 26 de octubre de 2017. Se recomienda al respecto dar mayor celeridad a la suscripción de las actas.

Función 5. Se observó que en cada una de las actas se dejó evidencia de los compromisos que se establecieron y del cumplimiento de los mismos. Se observó que en el documento Powerpoint que se presentó al comité, se incluyó la siguiente información respecto a cada compromiso del comité: actividad a realizar, fecha de realización, responsable, fecha de cumplimiento, observaciones de su seguimiento a la fecha de realización del comité y el estado del compromiso.

Función 6. Se observó mediante la verificación de correos electrónicos, presentaciones y documentos soporte, que se puso en conocimiento de los integrantes del comité para su revisión, comentarios y aprobación los documentos del subsistema de gestión de seguridad de la información y del subsistema de gestión de continuidad de negocio.

5.4 Verificación del estado de las acciones de mejora asociadas a las funciones del Comité de Seguridad de la Información y Continuidad de Negocio

El proceso Gestión integral de riesgo tiene en proceso las siguientes acciones de mejora relacionadas con las funciones del Comité de Seguridad de la Información y Continuidad de Negocio:

Tabla 2. Estado de las acciones de mejora asociadas

Acción	Descripción	Observación OCI
PDA-2017-1En proceso	No se evidenció que en los comités de seguridad de la información y continuidad de negocio desarrollados el 2 de agosto y el 28 de septiembre de 2016 se haya realizado seguimiento a los programas periódicos de ejercicios y pruebas de la infraestructura tecnológica y continuidad de negocio	Se establecieron 6 acciones del plan de acción, de las cuales se han completado 5 al 100%, quedando pendiente la actividad Realizar el seguimiento y aprobación de las pruebas funcionales durante la(s) sesión(es) del Comité durante el segundo semestre. Avance 83%. Finaliza el 29/12/2017.
PDA-2017-7En proceso	Se evidenciaron falencias respecto al procedimiento: "Gestión de Accesos", específicamente en los ítems que hacen referencia al envío y entrega de credenciales a los nuevos usuarios, se evidenció que las credenciales se envían en texto plano y en archivos .doc, sin protección, las mismas también se envían con copia a los Jefes de Área o solicitantes. Se evidenciaron cuentas activas de Funcionarios y Contratistas, que tienen la fecha de caducidad errónea de acuerdo a las condiciones establecidas en el contrato y/o forma de vinculación. De igual manera se observaron cuentas que no tienen caducidad, y por su condición, deben tener una fecha de expiración de acuerdo al tiempo que van a permanecer laborando y/o prestando sus servicios a la Unidad	Las actividades asociadas al plan de acción son 18, de las cuales siete se han completado al 100%. Avance 43%. Finaliza el 18/12/2017.
PDA-2017-125 En proceso	Se presentó incumplimiento de la meta establecida del indicador "*Cumplimiento en la instrumentalización de controles de seguridad de la información*"	El plan de acción cuenta con siete actividades, de las cuales cinco se han completado al 100%. El incumplimiento del indicador continúa. Avance 7%. Finaliza el 31/12/2017.

Acción	Descripción	Observación OCI
PDA-2017-207 En proceso	Se observó que los resultados de ejercicios y pruebas a los planes de continuidad no fueron publicados en el aplicativo SGI (Responsable Oficial de Continuidad) ni divulgados, de acuerdo con lo establecido en el Procedimiento ejercicios y pruebas código 02-03-PR-05 v1, actividad 5 "Publicar y Divulgar", que indica "Aprobados los documentos de las pruebas estos deben publicarse en el SGI y divulgarse a los diferentes niveles de la UAECD".	El plan de acción tiene definidas cuatro actividades, de las cuales dos se han completado al 100%, quedando pendiente la socialización del resultado de ejercicios y pruebas a los responsables de procesos, líderes de continuidad de la Unidad y a los equipos de trabajo. Avance 50%. Finaliza el 28/11/2017.

Fuente: Aplicativo ISODOC

5.5 Verificación de la aplicación de los controles de los riesgos identificados

Se realizó la verificación de la efectividad de los controles establecidos para los riesgos identificados relacionados con Seguridad de la información y Continuidad de negocio del proceso Gestión Integral de Riesgos:

Tabla 3. Verificación de los controles establecidos para los riesgos identificados

Proceso	Riesgo identificado	Controles establecidos	Observación OCI
Gestión Integral de Riesgos, Subproceso Seguridad de la información	Posible atención inadecuada del incidente de seguridadreportado.	Realizar sesiones para revisión del estado de ejecución de los planes de trabajo.	El riesgo se encuentra en zona inherenteMODERADO. Se evidenció que el control se está aplicando, a partir de los seguimientos realizados por la Oficial de cumplimiento con funcionarios de la Gerencia de Tecnología.

Fuente: Mapa de riesgos del proceso

CONCLUSIONES

A partir de los resultados de este informe, se observó que el Sistema de Control Interno del Comité Seguridad de la información y Continuidad de Negocio de la UAECD en el período comprendido entre el 1 de junio de 2017 y el 31 de octubre de 2017 es adecuado.

Los resultados de este informe y las evidencias obtenidas de acuerdo con los criterios definidos, se refieren sólo a los documentos examinados y no se hacen extensibles a otros soportes.

MEMORANDO

RECOMENDACIONES

- Acoger la solicitud de la Secretaria Técnica del Comité, en cuanto a una mayor participación en la revisión de los documentos que se someten a revisión y aprobación por parte de los integrantes del Comité.
- Dejar explícito en las Actas que se sometió a consideración del comité la aprobación de políticas, planes, documentos y demás información relacionada con el cumplimiento de las funciones del Comité.
- Dar mayor celeridad a la suscripción de las actas del Comité.
- Continuar con la aplicación del autocontrol y autorregulación en el desarrollo de las actividades asociadas al desarrollo de las funciones del Comité de Seguridad de la Información y Continuidad de Negocio.

Agradecemos a los integrantes del Comité de Seguridad de la Información y Continuidad de Negocio informar a la Oficina de Control Interno sus observaciones respecto al contenido del presente informe, a los correos avillamil@catastrobogota.gov.co y ayomayuza@catastrobogota.gov.co, a más tardar el viernes 25 de noviembre de 2017.

Cordialmente,

ALBA ENIDIA VILLAMIL MUÑOZ
Jefe Oficina de Control Interno

Copia: Orlando José Maya Martínez – Jefe Oficina Asesora de Planeación y Aseguramiento de Procesos
Eliécer Vanegas Murcia – Gerente de Tecnología
Olga Lucía López Morales – Gerente de Información Catastral
Sandra Patricia Samacá Rojas – Gerente IDECA
Ligia Elvira González Martínez – Gerente Comercial y de Atención al Usuario
Andrés Fernando Agudelo Aguilar – Gerente Gestión Corporativa
Tania Barrera Rodríguez – Oficina Seguridad de la Información - Secretaria Comité SICN
José Abraham Villarraga Ríos – Oficial de Continuidad de Negocio

Elaboró: Alexandra Yomayuza C. – Profesional Especializado OCI