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

UNIDAD ADMIN. CATASTRO DISTRITAL 18-11-2016 03:16:43
Al Contestar Cite Este Nr.:2016IE15082 O 1 Fol:1 Anex:0
ORIGEN: Origen: OFICINA DE CONTROL INTERNO/VILLAMIL MUÑOZ AL
DESTINO: Destino: DIRECCION GENERAL/PUENTES RIAÑO CLAUDIA CI
ASUNTO: Asunto: INFORME DE SEGUIMIENTO AL COMITÉ DE SEGURIC
OBS: Obs.:

MEMORANDO

Unidad Administrativa Especial de Catastro Distrital
DIRECCIÓN
18 NOV 2016
RECIBIDO
HORA: 3:40 p.m.

Referencia: Plan Operativo Anual de la OCI vigencia 2016

Fecha : 18 de noviembre de 2016

PARA : Claudia Puentes Riaño
Directora General 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 de la UAECD para el período comprendido entre el 20 de junio a 31 de octubre de 2016

Cordial Saludo Dra. Claudia:

En desarrollo del Plan Operativo Anual de la Oficina de Control Interno establecido para la vigencia 2016, la Oficina de Control Interno realizó seguimiento al Comité Seguridad de la Información y Continuidad de Negocio de la Unidad, de acuerdo con lo dispuesto en la Resolución 2806 de 2015, para el período comprendido entre el 20 de Junio de 2016 hasta el 31 de octubre de 2016, con la finalidad de contribuir al fortalecimiento del Sistema de Control Interno y el mejoramiento continuo a partir de la identificación de oportunidades de mejora y/o recomendaciones.

1. OBJETIVO GENERAL

Realizar seguimiento al cumplimiento de las disposiciones vigentes relacionadas con el Comité Seguridad de la información y continuidad de negocio de la Unidad.

2. OBJETIVOS ESPECÍFICOS

- Verificar el cumplimiento de las disposiciones contenidas en la Resolución 2806 de 2015.
- Verificar el cumplimiento de los compromisos adquiridos por el Comité de Seguridad de la Información y Continuidad de Negocio.
- Verificar el estado de las acciones de mejora asociadas al Comité de Seguridad de la Información y Continuidad de Negocio.
- Verificar la gestión de riesgos asociados a las funciones del Comité.

3. ALCANCE

Comités desarrollados en el período comprendido entre el 20 de Junio de 2016 y el 31 de octubre de 2016

4. MARCO NORMATIVO

Decreto 1083 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública*", Artículo 2.2.21.6.1 mediante el cual se adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano (MECI).

5. METODOLOGÍA

La verificación se realizó dentro del marco de las normas de auditoría generalmente aceptadas (NAGAS), e incluyó: la planeación, el análisis de la normatividad vigente, los procedimientos y demás documentación asociada; la verificación de la información suministrada por la Gerencia de Tecnología y la elaboración del informe con las conclusiones y recomendaciones, con el fin de mejorar el sistema de control interno de la Unidad.

6. PRESENTACIÓN DE RESULTADOS

6.1 Verificación del cumplimiento de las disposiciones contenidas en la Resolución 2806 de 2015

6.1.1. 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 dos sesiones del Comité de Seguridad de la Información y Continuidad de Negocio en el período evaluado como se indica a continuación:

Acta No. 03 del 2 de agosto de 2016.
La reunión fue convocada por la Secretaria Técnica del Comité, el 26 de julio de 2016. Se evidenció que se convocó a: la Directora de la UAECD, Gerente de Información Catastral, Gerente Comercial y de Atención al Usuario, Gerente Corporativa, Gerente Ideca (e), Gerente de Tecnología, Jefe Oficina Asesora de Planeación, Oficial de Seguridad de la Información, Oficial de Continuidad de Negocio, Jefe Oficina Asesora Jurídica, Jefe Control Interno, Asesor de Comunicaciones, Subgerente de Ingeniería de Software, Asesora de la Gerencia Catastral.

Asistieron a la reunión los siguientes miembros permanentes: La Directora de la Unidad, el Gerente de Infraestructura de Datos Espaciales-IDECA (e), la Gerente Corporativa, el Gerente de Tecnología, el Jefe de la OAPAP y la Oficial de seguridad de la información. Además, asistieron como invitados: la Jefe de la Oficina de Control Interno, un (1) profesional de la Oficina Asesora Jurídica, y el Asesor de Comunicaciones de la Dirección. Según los formatos de control de asistencia evidenciados, se observó, que en la reunión efectuada el 2 de agosto de 2016 (acta N° 3) se conformó quórum decisorio, cumpliendo con lo dispuesto en los artículos 4 y 5 de la Resolución 2806 de 2015.

Acta No. 04 del 28 de septiembre de 2016.

La reunión fue convocada por la Secretaria Técnica del Comité, el 13 de septiembre de 2016. Se evidenció que se convocó a: la Directora de la UAECD, Gerente de Información Catastral, Gerente Comercial y de Atención al Usuario, Gerente Corporativa, Gerente Infraestructura de Datos Espaciales - IDECA, Gerente de Tecnología, Jefe Oficina Asesora de Planeación, Oficial de Seguridad de la Información, Oficial de Continuidad de Negocio, Jefe Oficina Asesora Jurídica, Jefe Control Interno, Asesor de Comunicaciones, Asesora de la Gerencia Catastral.

Asistieron a la sesión los siguientes miembros permanentes: La Directora de la Unidad, la Gerente Corporativa (quien actuó también como Gerente de Infraestructura de Datos Espaciales - IDECA(e), el Gerente de Tecnología, la Gerente Comercial y de atención al usuario, el Jefe de la OAPAP, el Oficial de Continuidad de negocio y la Oficial de seguridad de la información. Además, asistieron como invitados: la Jefe de la Oficina de Control Interno, la Subgerente de Recursos Humanos, una (1) profesional de la Subgerencia de Recursos Humanos y el Asesor de Comunicaciones de la Dirección. Según los formatos de control de asistencia evidenciados, se observó, que en la reunión efectuada el 28 de septiembre de 2016 (acta N° 4) se conformó quórum decisorio, cumpliendo con lo dispuesto en los artículos 4 y 5 de la Resolución 2806 de 2015.

Se observó que en el período objeto de seguimiento no se convocaron reuniones extraordinarias del Comité de Seguridad de la Información y Continuidad de Negocio.

6.1.2 Verificación del cumplimiento de las funciones definidas para el Comité

Las funciones definidas para el Comité de Seguridad de la Información y continuidad de negocio se encuentran definidas en el artículo 3° de la Resolución 2806 de 2015:

"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 que durante el período comprendido entre el 20 de Junio hasta el 31 de octubre de 2016, se desarrollaron las siguientes funciones del Comité, de acuerdo con los registros consignados en las Actas 3 y 4 de 2016:

Función 1. Se presentó la Estrategia Institucional de Respuesta a Emergencias (acta 4 numeral 2.1.1).

Función 2. Se revisó la política de seguridad de la información en cumplimiento de lo dispuesto en la Resolución 305 de 2008, quedando registrado en el Acta 3 numeral 3: "*El comité confirma durante la presente sesión que dichas políticas no requieren ajustes y se mantiene la versión actual de la misma, publicada en el manual del SGSI*". Se aprobaron por parte del Comité los siguientes documentos: Encuesta SGSI, Estratificación SGSI, Equipo operativo de continuidad de negocio (Acta 3 numeral 3).

Función 3. Se aprobó por parte del Comité el Plan de implementación presentado para la "habilitación de la regla adicional para restringir la instalación de software a través del software Symantec" (acta 3 numeral 2.2) y se continúa con la revisión de la Política de datos personales, frente a la cual ya se pronunció la Oficina de Control Interno (acta 4 numeral 3).

Función 4. Se evaluó la ubicación de los roles de Oficial de Seguridad de la Información y el Oficial de Continuidad de negocio, y se decidió su traslado a la OAPAP, quedando como uno de los compromisos del acta 4 (acta 4 numeral 3).

Función 5. Se presentó al Comité la propuesta de integrantes del Grupo Operativo de Continuidad de Negocio y se solicitó a la Subgerencia de Recursos Humanos el listado de personas que asistieron a los cursos de seguridad de la información, quienes podrán apoyar en la ejecución de las actividades establecidas en el plan de trabajo para este segundo semestre.

Función 6. Se fijó como compromiso del acta No. 4 la revisión del documento de protocolo de la EIRE (acta 4 numeral 3), se conformó el grupo operativo de continuidad del negocio y se encuentra en revisión el acto administrativo correspondiente (acta 4 numerales 2.1.2 y 3).

Función 7. Se aprobó el plan de trabajo del segundo semestre de 2016, el cual incluye actividades relacionadas con la actualización al SGSI y al SGCN, tales como el plan de transición de IPv4 a IPv6 (Acta 3 numeral 2.3).

Función 11. Se presentó en Comité del 2 de agosto de 2016, la relación de 9 incidentes de seguridad de la información presentados entre febrero y julio de 2016 (Presentación acta 3).

Función 12. Se aprobó el plan de trabajo para la apropiación del sistema de gestión de seguridad de la información para el segundo semestre de 2016 (Acta 3 numeral 2.3).

Función 13. Se aprobó el plan de trabajo del segundo semestre de 2016, el cual incluye actividades relacionadas con la ampliación del alcance del SGSI y la alineación con el SGI.

Se observó que durante el período comprendido entre el 20 de junio de 2016 y el 31 de octubre de 2016, el Comité de Seguridad de la Información y Continuidad del Negocio no realizó el seguimiento a los *"programas periódicos de ejercicios y pruebas de la infraestructura tecnológica y continuidad de negocio"*, tal como se establece en el numeral 11 del artículo 3° de la Resolución 2806 de 2015.

(AC) 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,

incumpliendo lo dispuesto en el numeral 11 del artículo 3° de la Resolución 2806 de 2015: "*FUNCIONES. El Comité del que trata el presente acto administrativo ejercerá las siguientes funciones: ... 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...*", así como lo establecido en el elemento 1.2.5 Políticas de Operación de MECI:2014, en el entendido que "*define los límites y parámetros necesarios para ejecutar los procesos y actividades en cumplimiento de la función, los planes, los programas, proyectos y políticas de administración del riesgo y de otros procesos previamente establecidos por la entidad*".

6.1.3 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

Se observó que la Secretaria Técnica del Comité (Oficial de Seguridad de la Información) realizó la citación a los integrantes del mismo con la debida anticipación mediante correos electrónicos del 26 de julio y 13 de septiembre de 2016 y remitió la agenda propuesta.

Se evidenció que se elaboró y se encuentra suscrita el Acta No. 3 del Comité. En cuanto al Acta No.4 del comité realizado el 28 de septiembre, se observó que se puso a disposición de los integrantes del comité el 3 de noviembre, por tanto a la fecha del seguimiento no se encontraba aprobada ni suscrita.

Al respecto, se recomienda dar mayor celeridad a la suscripción de las actas del comité, en cumplimiento de lo establecido en la función 4 del Secretario Técnico del Comité (artículo 8 de la Resolución 2806 de 2015) y el parágrafo del artículo 6 de la Resolución 2806 de 2015.

Se observó que incluyó en cada una de las reuniones, un punto relacionado con el seguimiento a los compromisos previos, el cual hace parte de la presentación de Power point de cada sesión. Al respecto, en

el numeral 6.2 de este informe, se presenta el seguimiento al cumplimiento de dichos compromisos, realizado por la OCI.

Se observó mediante la verificación de correos electrónicos, presentaciones y documentos soporte, que puso en conocimiento de los integrantes del comité, los siguientes documentos para su revisión y comentarios: Revisión de los protocolos identificados dentro del Plan de Emergencias de Bogotá (PEB), Política de Control de Acceso.

6.2 Verificación del cumplimiento de los compromisos del Comité de Seguridad de la información y Continuidad de Negocio en el período 20 de junio a 31 de octubre de 2016

El artículo 8° de la Resolución 2806 de 2015 dispone respecto a las funciones del Secretario Técnico del Comité, en su numeral 5. *Verificar el cumplimiento de las decisiones adoptadas en el seno de las reuniones.*

Situación evidenciada

Se evidenció que en cada una de las sesiones del Comité, se realizó seguimiento a los compromisos del comité anterior. Al respecto, esta Oficina observó frente a las fechas de ejecución de los compromisos establecidos, las siguientes situaciones:

Compromisos Actas Comité de Convivencia Laboral 2016			
Compromiso registrado en el Acta	**Responsable**	**Fecha programada / cumplimiento**	**Observaciones OCI**
Compromisos Acta No. 3			
Presentar mejores prácticas respecto al área a la que debe pertenecer el Oficial de Seguridad de la Información y el Oficial de Continuidad del Negocio.	Gerencia de Tecnología	13-09-2016 / 28-09-2016	Se observó en acta No. 4 del Comité del SICN que el tema fue presentando al comité reunido el 28 de septiembre de 2016.
Realizar la publicación del formato actualizado "Formato de constancia para entrega de bienes y/o elementos asignados y documentos".	Subgerencia Administrativa y Financiera	31-08-2016 / 20-09-2016	Se verificó en ISODOC que el formato fue actualizado y publicado con el código 10-101-FR-01 v7.
Revisar el texto a incluir en el formato "Formato de constancia para entrega de bienes y/o elementos asignados y documentos" para contemplar la entrega adecuada de las supervisiones y quien actuaría como verificador del cumplimiento de dicha entrega.	Subgerencia Administrativa y Financiera	06-09-2016 / 20-09-2016	Se verificó en ISODOC que el formato fue actualizado y publicado, e incluye la siguiente nota: "*El Servidor o contratista que se desvincula de la Entidad debe obtener la firma de cada verificador con la que se constata que el(los) bien(es) o elementos o documentos han sido entregados a la Entidad. Una vez diligenciado este documento debe radicarlo en Correspondencia para su posterior entrega en la Subgerencia de Recursos Humanos (para servidores públicos) para que repose en la respectiva historia laboral o en la Oficina Asesora Jurídica (para contratistas) para que repose en la carpeta del contrato que corresponda*".

MEMORANDO

Compromisos Actas Comité de Convivencia Laboral 2016			
Compromiso registrado en el Acta	**Responsable**	**Fecha programada / cumplimiento**	**Observaciones OCI**
Ajustar política de protección de datos personales para revisión de la Oficina Asesora Jurídica, la cual se realizará una vez se cuente con el procedimiento de datos personales (Consulta y reclamación).	Gerencia de Tecnología Gerencia Comercial y de atención al usuario	09-09-2016 / 16-09-2016	Se observó que la Política de protección de datos personales fue revisada por la Gerencia Comercial y de Atención al Usuario el 16 de septiembre y remitida a la GT mediante correo electrónico.
Generar el procedimiento de datos personales (Consulta y reclamación)	Gerencia de Tecnología Gerencia Comercial y de atención al usuario	11-11-2016	De acuerdo con la consulta realizada en ISODOC, el procedimiento "*Consulta y reclamación de datos personales*" se encuentra en etapa de elaboración.
Realizar revisión de la propuesta de resolución para la conformación del grupo de continuidad del negocio de la UAECD, previa remisión de la misma por parte de la Gerencia de Tecnología y dentro de los plazos que indiquen las disposiciones legales.	Oficina Asesora Jurídica	13-09-2016 / Al corte del 31 de octubre no se había culminado esta actividad	El 7 de septiembre de 2016 se envió propuesta de resolución a la Oficina Asesora Jurídica. El 13 de octubre el abogado de la OAJ manifestó que tenía algunas observaciones de fondo y de forma sobre el proyecto y solicitó reunión en esa misma fecha.
Generar nueva comunicación a la Alta Consejería de TIC, solicitando una reunión formal de aclaraciones del modelo por parte del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC	Gerencia de Tecnología	13-09-2016	No se generó la comunicación. De acuerdo con lo informado por la Gerencia de Tecnología, "No se requiere nueva comunicación, puesto que las observaciones realizadas al Modelo fueron tenidas en cuenta para la versión que recién fue publicada en el portal de MINTIC. Se acuerda generar comunicación confirmando que la UAECD continuará con el modelo de MINTIC anterior". Se verificó comunicación enviada a la Alta Consejería de las TIC radicada con cordis 2016EE57037
Revisar estrategia para publicación del formato "Instrumento de Gestión de Información Pública", ya se dicho formato contiene los campos solicitados durante la caracterización documental.	OAPAP Gestión documental, Gerencia de Tecnología	13-09-2016 / 27-09-2016	Se verificó en ISODOC la publicación del formato "Instrumento de Gestión de Información Pública", con código 13-133-FR-5 v1, asociado al subproceso de gestión de seguridad de la informaciónel 27 de septiembre de 2016.
Validar si es posible identificar los usuarios que generaron certificaciones que figuran como expedidas a nombre de … (incidente SOL095966-16).	Gerencia de Tecnología	13-09-2016 / 29-08-2016	Se observó la respuesta suministrada mediante el ticket N°. SOL098945-16, donde se anexan dos archivos con el detalle de las certificaciones generadas en las cuales aparece registrado en el SIIC el usuario de la funcionaria registrada en el incidente SOL095966-16

MEMORANDO

Compromisos Actas Comité de Convivencia Laboral 2016			
Compromiso registrado en el Acta	**Responsable**	**Fecha programada / cumplimiento**	**Observaciones OCI**
Generar listado de carpetas compartidas y los accesos autorizados a las mismas para validación de las dependencias.	Gerencia de Tecnología	13-09-2016 / Al corte del 31 de octubre no se había culminado esta actividad	Se evidenció el listado de carpetas compartidas de la Gerencia Comercial y de Atención al Usuario, de fecha 27 de octubre de 2016. No se observa información de otros procesos o dependencias.
Solicitar a Gestión Humana el listado de personas que asistieron a los cursos de seguridad de la información, quienes podrán apoyar en la ejecución de las actividades establecidas en el plan de trabajo para este segundo semestre.	Gerencia de Tecnología	13-09-2016 / 24-08-2016	Se verificó la información remitida por la profesional a cargo de las capacitaciones en la Subgerencia de Recursos Humanos, respecto a los asistentes al curso de auditor ISO 27001 el 24 de agosto de 2016.
Compromisos Acta No. 4			
Revisar documento de protocolo de la EIRE y enviar observaciones a José Villarraga.	Integrantes Comité e invitados	14-10-2016 / 07-10-2016	El documento fue observado por el Jefe de la OAPAP y la Jefe de la OCI con fechas 7 de octubre y 4 de octubre respectivamente. No se observan comentarios de los demás integrantes del Comité.
Enviar matriz de turnos de la EIRE	Shirlei Pimiento Ortega	2016-09-28 / No se evidenció que se haya adelantado esta actividad	Al corte del 31 de octubre no se evidenció que se haya adelantado esta actividad
Diligenciar/actualizar matriz de turnos de la EIRE	Integrantes Comité e invitados	2016-10-03 / No se evidenció que se haya adelantado esta actividad	Al corte del 31 de octubre no se evidenció que se haya culminado esta actividad
Agendar para noviembre reunión con IDIGER durante próximo Comité	Shirlei Pimiento Ortega y José Abraham Villarraga	Próximo Comité	Se evidenció correo remitido a Idiger el 3 de noviembre por parte del Oficial de Continuidad de Negocio, solicitando una charla de 40 minutos el 17 de noviembre de 2016.
Revisar reasignación de área responsable para liderar la EIRE en la Unidad y presentar propuesta.	Orlando José Maya Martínez	Próximo Comité	Al corte del seguimiento, no se observó avance respecto a esta actividad.
Revisar los integrantes del grupo operativo con las dependencias correspondientes, indicando el cargo y validar la aplicación de la	José Abraham Villarraga	Próximo Comité	Al corte del seguimiento, no se observó avance respecto a esta actividad.

Compromisos Actas Comité de Convivencia Laboral 2016			
Compromiso registrado en el Acta	**Responsable**	**Fecha programada / cumplimiento**	**Observaciones OCI**
estrategia de teletrabajo.			
Generar comunicación a la Dirección solicitando actualización en el manual de funciones y movimiento de los cargos asociados al rol de Oficial de Seguridad de la Información y rol de Oficial de Continuidad del Negocio de la Gerencia de Tecnología a la OAPAP, para que su gestión ante la Comisión Nacional del Servicio Civil	Tania Barrera Rodríguez	15-10-2016 Al corte del 31 de octubre no se había culminado esta actividad	Se observó borrador de la solicitud a realizar a la Directora de la Unidad, solicitando la actualización del manual, así como el borrador de la plantilla de funciones de los cargos Profesional Especializado 222-10 y 222-11 quienes ofician como Oficial de seguridad de la información y Oficial de Continuidad de negocio respectivamente.
Revisar política de datos personales la cual contiene textos en morado para concepto al respecto por parte de la Oficina de Control Interno.	Alba Enidia Villamil	30-09-2016 / 03-10-2016	Se observó que mediante correo electrónico se recomendó por parte de la Jefe de la OCI tener en cuenta las disposiciones vigentes, por tanto no aplica la salvedad respecto a que "*no deberá ser objeto de ningún tipo de auditoría*" los textos identificados en color morado dentro del documento.
Generar comunicación a la Alta Consejería confirmando que la UAECD continuará con el modelo de MINTIC anterior para avanzar en las demás fases del modelo.	Tania Barrera Rodríguez	Próximo Comité	Se evidenció oficio remitido al Alto consejero Distrital de TIC el 8 de noviembre de 2016 radicado con cordis 2016EE57037, informando que "*...el Comité de Seguridad de la Información y Continuidad de Negocio en su reunión No. 4 del 28 de septiembre de 2016, acordó que para evitar reprocesos, reducir el impacto que estos cambios permanentes pueden generar y permitir avanzar en el plan de trabajo establecido durante el primer semestre, la Unidad continuará bajo su modelo aprobado en abril de 2016, alineado con la versión 3.0.0 del Modelo de seguridad y privacidad de la información de MINTIC*".

Se observó que no se han cumplido en la fecha programada el 55% de los compromisos fijados (11 del comité 3 y 9 del Comité 4), por tanto recomienda esta Oficina que se identifiquen las razones que conllevan a esta situación, para evitar que se siga repitiendo.

6.3 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 Provisión y soporte de servicios TI tiene en proceso las siguientes acciones de mejora relacionadas con las funciones del Comité de Seguridad de la Información y Continuidad de Negocio:

PDA-2016-694 - Derechos de Autor Instalación de Software no autorizado
PDA-2016-653 - Gestión de accesos para la definición de estándares de desarrollo seguro
PDA-2016-650 - Gestión de accesos sobre los aplicativos LPC, SICAPITAL, Catastro en Línea y SIIC
PDA-2016-647 - Incidente de seguridad de la información por el envío de un correo masivo
PDA-2016-646 - Incidente de seguridad de la información por la pérdida de la información de negocio
PDA-2016-645 - Incidente de seguridad de la información por la pérdida de la información de negocio
PDA-2015-393 - Incumplimiento del Control A.12.6.1 Control de vulnerabilidades Técnicas
PDA-2015-392 - Falencias respecto al procedimiento: "Gestión de Accesos"
PDA-2015-391 - Incumplimiento del Control A.10.5.1 Back-up o respaldo de la información
PDA-2015-389 - No se evidenciaron registros de auditorías periódicas de sistemas
PDA-2015-383 - Documentar el backup de computadores
PDA-2015-380 - Incumplimiento del Control A.7.2.1, Lineamientos de Clasificación

Se verificó en ISODOC- Módulo de mejoramiento continuo, la ejecución de las actividades asociadas a cada una de las PDA estado "en proceso", encontrando que para el período comprendido entre el 20 de junio y el 31 de octubre se han ejecutado en los plazos establecidos.

6.4 Verificación de la gestión de riesgos asociados a las funciones del Comité

6.4.1 Subproceso Gestión de continuidad

Riesgo: Posible ejecución o respuesta inadecuada del plan de continuidad en un evento real

Los controles asociados a este riesgo son los siguientes: *"Realizar pruebas periódicas de acuerdo a los planes de continuidad y definir planes de mejoramiento"*, *"Ejecutar el plan de sensibilización de los planes de continuidad a nivel operativo y administrativo"*, *"Actualización de los planes de continuidad periódicamente"*, *"Revisión y/o actualización del análisis de impacto al negocio y del análisis de riesgos periódicamente y Asegurar la asignación presupuestal apropiada y realizar el respectivo seguimiento"*.

La Gerencia de Tecnología definió 9 actividades en el plan de manejo de riesgos, las cuales al corte del tercer trimestre reportaron un avance del 94% frente a lo esperado en dicho período, ya que de acuerdo con lo informado por el Gerente de Tecnología *"El porcentaje restante se debe a que el proceso de contratación de uso de la herramienta para el Sub-sistema de Gestión de Continuidad del negocio se encuentra en etapa precontractual (Adjudicación). Esta actividad se debía cumplir este trimestre, se realizará seguimiento en el último trimestre"*. El contrato en mención fue adjudicado y se encuentra en ejecución desde el 12 de octubre de 2016.

6.4.2 Subproceso Gestión de seguridad de la información

Riesgo: Posible pérdida o robo de información del negocio

Los controles establecidos para evitar la materialización de este riesgo son: Copias de respaldo (A.12.3. ISO27001), Monitoreo sobre la infraestructura que soporta los activos de información (A.12.4.1. ISO27001), Mantenimiento de equipos (A.11.2.4 ISO27001), Procedimiento de gestión de incidentes (A.16.1 ISO27001), Verificada y probada la configuración adecuada, con base en los requerimientos de la UAECD, de los equipos de seguridad, Responsabilidad de los activos, Clasificación de la información,

Manejo de medios, Logs de auditorías sobre los sistemas de información, Gestión de vulnerabilidades técnicas, Toma de conciencia, educación y formación en la seguridad de la información (A.7.2.2 ISO27001).

El Plan de manejo de riesgos tiene definidas 22 actividades, con un avance del 95% en el tercer trimestre de 2016. De acuerdo con lo informado por el Gerente de Tecnología "*el porcentaje restante se debe a que se inició la verificación de las auditorias habilitadas en los diferentes sistemas de información, sin embargo no se concluyó dicha actividad. Se realizará seguimiento en el último trimestre*".

Riesgo: Posible pérdida de la confidencialidad y/o integridad de la información

Los controles establecidos son: Política de control de acceso (A.9 ISO27001), Procedimiento de control de acceso (A.9 ISO27001), Revisiones de los derechos de acceso de usuarios (A.9 ISO27001), Revisión del software instalado vs el software autorizado, Procedimiento de gestión de incidentes, Protección contra códigos malicioso (A.12.2), Control de software operacional (A.12.5), Restricciones sobre instalación de software (A.12.6.2), Derechos de propiedad intelectual (A.18.1.2), Responsabilidad de los activos, Clasificación de la información, Manejo de medios, Logs de auditorías sobre los sistemas de información, Gestión de vulnerabilidades técnicas (A.12.6.1), Transferencia de información (A.13.2), Copias de respaldo (A.12.3. ISO27001), Toma de conciencia, educación y formación en la seguridad de la información (A.7.2.2 ISO27001).

El Plan de manejo de riesgos establecido se compone de 30 actividades, las cuales en el tercer trimestre de 2016 presentaron un avance del 94%. De acuerdo con lo informado por el Gerente de Tecnología: "*El porcentaje restante se debe a que al momento de publicar la Política de Control de Acceso en el Sistema Integrado de Gestión - SGI la Oficina Asesora de Planeación y Aseguramiento de Procesos - OAPAP y la Oficina de Control Interno - OCI emitieron recomendaciones, se realizará el ajuste y publicación en el último trimestre del año. Adicionalmente se debe a que se inició la verificación de las auditorias habilitadas en los diferentes sistemas de información, sin embargo no se concluyó dicha actividad. Se realizará seguimiento en el último trimestre*". Al corte del seguimiento realizado por la OCI, el documento no se encuentra publicado ni actualizado en ISODOC.

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 20 de junio de 2016 y el 31 de octubre de 2016 es susceptible de mejora.

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.

RECOMENDACIONES

- Implementar la acción correctiva relacionada con el cumplimiento de las funciones asignadas al Comité mediante la Resolución 2806 de 2015, en cuanto a 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.

MEMORANDO

- Dar mayor celeridad a la suscripción de las actas del comité y realizar seguimiento al cumplimiento de los compromisos establecidos en las actas de comité, en las fechas programadas.
- Continuar con la aplicación del autocontrol y autorregulación en el desarrollo de las actividades asociadas al 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 hallazgo y recomendaciones presentados en este informe, a los correos avillamil@catastrobogota.gov.co y ayomayuza@catastrobogota.gov.co, a más tardar el día 25 de noviembre de 2016 y en caso de requerirse, se realice una mesa de trabajo para analizar e identificar la causa raíz y definir el plan de acción que permita su eliminación. Si en la fecha mencionada no se han recibido observaciones, se entenderá en firme el informe y se procederá al registro de la acción preventiva en el aplicativo ISODOC.

Cordialmente,

ALBA ENIDIA VILLAMIL MUÑOZ
Jefe Oficina de Control Interno

Copia: Sandra Patricia Samacá Rojas – Gerente de Información Catastral
Olga Lucía López Morales - Gerente Corporativa y Gerente IDECA (E)
Ligia Elvira González Martínez – Gerente de Comercialización y Atención al Usuario
Eliécer Vanegas Murcia – Gerente de Tecnología
Orlando José Maya M. – Jefe Oficina Asesora de Planeación y Aseguramiento de Procesos
Tania Barrera R. – Oficial de Seguridad de la Información
José A. Villarraga R. – Oficial de Continuidad de Negocio

Elaborado y verificado por: Alexandra Yomayuza C.