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

UNIDAD ADMIN. CATASTRO DISTRITAL 08-08-2018 11:08:50
Al Contestar Cite Este Nr.:2018IE11706 O 1 Fol:1 Anex:0
ORIGEN: Origen: Sd:141 - OFICINA DE CONTROL INTERNO/NAVAS FLO
DESTINO: Destino: DIRECCION GENERAL/AGUDELO AGUILAR ANDRES
ASUNTO: Asunto: SEGUIMIENTO COMITE DE SEGURIDAD DE LA INFOR
OBS: Obs.: PTROYECTO / DANILO BAQUERO

MEMORANDO

Unidad Administrativa Especial de Catastro Distrital
DIRECCIÓN
08 AGO 2018
RECIBIDO
HORA: 2:32

Referencia: Plan Anual de Auditoria vigencia 2018

Fecha: 08 de Agosto de 2018

PARA: Andrés Fernando Agudelo Aguilar
Director (E) - Unidad Administrativa Especial de Catastro Distrital

DE: Johny Gender Navas Flores
Jefe Oficina de Control Interno

ASUNTO: Seguimiento Comité de Seguridad de la Información y continuidad de Negocio - CSICN

Cordial saludo Dr. Agudelo.

En cumplimiento del Plan Anual de Auditorías de la OCI de la vigencia 2018, remito para su conocimiento y fines que considere pertinentes, Informe citado en el asunto. En cumplimento de la 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*". Directiva 003 de 2013 de la Alcaldía Mayor de Bogotá.

Cordialmente,

JOHNY GENDER NAVAS FLORES
Jefe Oficina de Control Interno

Copia: Orlando Maya Martínez – Jefe Oficina Asesora de Planeación y Aseguramiento de Procesos
Oswaldo Andrés González B – Jefe Oficina Asesora Jurídica
Mayiver Méndez Sáenz– Jefe Oficina Control Disciplinario
Sandra Patricia Samacá Gerencia IDECA
Pamela del Pilar Mayorga Ramos – Subgerencia de Operaciones.
Yenny Carolina Rozo Gómez –Subgerente de Información Física y Jurídica
Maria Isabel Cogua M. – Subgerente de Información Económica
Ligia Elvira González – Gerente de Comercialización y Atención al Usuario
Winston Darío Hernández P. – Subgerente Administrativo y Financiero
Rosalbira Forigua R. – Subgerente Recursos Humanos
José Luis Ariza V. - Gerente de Tecnología
Fredy Leonardo Varón G. – Subgerencia Ingeniería del Software.
Nancy del Pilar Valencia Trujillo - Subgerente de Infraestructura Tecnológica

Elaboró: Danilo Baquero Profesional Contratista – OCI.

ALCALDÍA MAYOR DE BOGOTÁ D.C. HACIENDA Unidad Administrativa Especial Catastro Distrital	**INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO**

Seleccionar tipo de Informe:

Evaluación [ ] Seguimiento [X] Auditoría de Gestión [ ]

NOMBRE DEL INFORME:

Seguimiento Comité de Seguridad de la Información y continuidad de Negocio - CSICN

1. OBJETIVO GENERAL

Realizar seguimiento a las funciones desarrolladas por 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 noviembre de 2017 y el 30 de junio de 2018.

3. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA

- 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".
- Directiva 003 de 2013 de la Alcaldía Mayor de Bogotá.

4. METODOLOGÍA

El seguimiento se realizó aplicando las normas internacionales de auditoría, lo cual incluye la planeación, ejecución, generación y comunicación del informe con las conclusiones y recomendaciones, que permitirán contribuir al mejoramiento del Sistema de Control Interno.

5. PRESENTACIÓN DE RESULTADOS

5.1 Verificación al cumplimiento del Comité de Seguridad de la Información y Continuidad de Negocio.

5.1.1 Conformación del CSICN de la Unidad.

Acorde con lo establecido en la Resolución 2806 de 2015 los artículos 4 "*Conformación del comité de seguridad de la información y continuidad de negocio...*" y mediante Cordis 2018IE10417 del 13 de julio de 2018, enviado por la Gerencia de Tecnología a la Oficina de Control Interno donde informó de como se encuentra conformado el CSICN y "*...quienes concurrirán como miembros permanentes, con voz y voto*" así:

- *El Director.*
- *El Gerente de Tecnología.*
- *El Gerente de Información Catastral.*
- *El Gerente de Gestión Corporativa.*
- *El Gerente de Infraestructura de Datos Espaciales (IDECA).*
- *El Gerente Comercial y de Atención al Usuario.*
- *El Jefe de la Oficina Asesora de Planeación y Aseguramiento de Procesos.*
- *El Oficial de Seguridad de la Información, adscrito a la Gerencia de Tecnología.*
- *El Oficial de Continuidad de Negocio, adscrito a la Gerencia de Tecnología.*

Artículo 5 Reuniones, 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."

Situación evidenciada

La OCI verificó las actas de CSICN entregadas por la GT (Oficial de Seguridad de la Información) donde el la Secretaría Técnica del Comité presentó funciones definidas mediante la Resolución 2806 de 2015, observando el cumplimiento de las mismas durante la vigencia del 01 de noviembre de 2017 al 30 de junio de 2018, dentro de las actividades se programaron y realizaron tres (3) sesiones del Comité generando los siguientes documentos: Actas No 7 Noviembre de 2017, Acta No 1 marzo 15 de 2018 y Acta N° 2 mayo 16 de 2018. A continuación Tabla No 1 se describe seguimiento a las sesiones del Comité de SICN

Tabla 1. Sesiones del CSICN noviembre 2017 – junio 2018

Acta	Fecha	Quórum	Asistencia	Temas tratados
Acta No. 7 Ordinaria	17 nov 2017	SI	Acorde con lo establecido en la Resolución N° 2806 de 2015 Articulo 4. ✓Director (E), ✓Gerentes (3), - Gerente de Tecnología - Gerente de Gestión Corporativa. - Gerente Comercial y de atención al usuario. ✓Jefe OAPAP ✓Oficial de Seguridad de la Información ✓Oficial de Continuidad del Negocio Invitados: Profesional especializado – OCI, Jefe Oficina Asesora Jurídica, Profesional Especializado – Comunicaciones.	Se realizó seguimiento a compromisos anteriores entre ellos. 1. Se observó que se llevó a cabo la presentación del CSICN sesión N° 7 de 2017. 2. Se definió Procedimiento de comunicación en caso de emergencia a elaborar por parte de la GT, OAPAP, SAF. 3. Necesidad de utilización de medios removibles CDs, DVDs, USB con las dependencias de la unidad.
Acta No. 1 Ordinaria	15 marzo 2018	SI	✓ Directora ✓ Gerentes (3) - Gerente de Tecnología - GT - Gerente de Gestión Corporativa. - Gerente de Infraestructura de Datos Espaciales - IDECA ✓ Jefe OAPAP ✓ Oficial de Seguridad de la Información ✓ Oficial de Continuidad del Negocio Invitados: - Subgerente Recursos Humanos - Profesional Especializado – Oficina Control Interno - OCI - Contratista – OCI. - Profesional Especializado – Oficina Asesora Jurídica - Contratista – GT - Consultores Consorcio Mnemo – SGSI.	✓Incidentes de seguridad de la información reportados: ✓Robo de memoria presentado piso once. ✓Malware minería de Criptomonedas ✓Mal uso de Internet Se propone socializar tema de la política de confidencialidad. • Guía para la implementación del principio de responsabilidad (datos personales de la unidad.) • Se presentó el documento para revisión y aprobación *"Declaración de aplicabilidad"* el cual lista los controles de seguridad de la información Acorde con el anexo A del estándar ISO/IEC 27001 V.2013. • Presentación de la consultoría Mnemo quienes llevarán el fortalecimiento del SGSI y actualización del SICN • Compromisos nuevos

Acta	Fecha	Quórum	Asistencia	Temas tratados
Acta N° 2 Ordinaria	16 mayo 2018	SI	Gerentes (5) - Gerente de Tecnología – GT - Gerente de Información Catastral - GIC - Gerente de Gestión Corporativa. - Gerente de Infraestructura de Datos Espaciales – IDECA - Gerente Comercial y de Atención al Usuario – GCAU ✓ Jefe OAPAP ✓ Oficial de Seguridad de la Información ✓ Oficial de Continuidad del Negocio Invitados: Subgerente de Infraestructura Tecnológica – SIT - Subgerente de Ingeniería del Software - Jefe Oficina Control Interno – OCI. - Contratista – OCI. - Jefe Oficina Asesora Jurídica - Contratista – GT - Consultores Consorcio Mnemo – SGSI.	Se presentó al comité documento *"plan de trabajo 2018 para implementación de controles ISO 27001"*contiene las actividades para implementar los controles de Seguridad de la Información el cual se enviará al contratista y recibir nuevas observaciones para aprobación del documento. Aprobación de tres documentos por la supervisión del contrato 191 de 2018. Levantamiento de activos de información se llevarán a cabo en el formato *"Instrumento de gestión de la Información Pública"* de este documento se retirara la sección *"esquema de publicación"* debido a que la OAPAP adoptó el esquema de publicación como acto administrativo independiente. Avance de la consultoría Mnemo anexo Técnico contrato 191-2018 fortalecimiento del SGSI y actualización SGCN.

Fuente: Elaboración propia auditor OCI actas de CSICN período comprendido entre el 1 de noviembre de 2017 y el 30 de junio de 2018

Situación Evidenciada:

Se Observó en los tres comités presentados en la vigencia del 1 de noviembre de 2017 al 30 de junio de 2018, que fueron convocados los miembros del CSICN acorde con lo establecido en la Resolución 2806 de 2015, artículos 4 y 5, adicional como invitados o participantes a las reuniones los jefes de la Oficina de Control Interno y Oficina Asesora Jurídica, Subgerente Infraestructura Tecnológica, Subgerente Ingeniería del Software, Contratistas y Consultoría Mnemo, Confirmando quórum decisorio.

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

Situación Evidenciada:

Acorde con lo establecido en la Resolución 2806 de 2015 artículo 8 *"Funciones del Secretario Técnico del Comité de Seguridad de la Información y de Continuidad de Negocio,"* A continuación vea tabla N° 2 Funciones Secretaria Técnica CSICN.

Tabla N° 2 Funciones Secretaria Técnica CSICN

Funciones del Secretario Técnico del CSICN	**Situación Evidenciada**
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.	Se observó que la (Oficial de Seguridad de la Información) lleva a cabo funciones como Secretaria Técnica del CSICN, quien efectuó citación a los integrantes del Comité, indicando la agenda a tratar. Se observó que en los comités realizados presentó los temas programados y acordes a la agenda propuesta.
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.	Se observó que la Secretaria Técnica del CSICN, envía a los integrantes del Comité la correspondiente información y temas a tratar durante las reuniones, acorde con lo establecido en la Resolución 2806 de 2015 Artículo 8°.
3. Velar por el buen funcionamiento del Comité.	Se observó que la Secretaria Técnica del CSICN, lleva a cabo la actividad acorde con lo establecido en la Resolución 2806 de 2015 Artículo 8° literal 3.
4. Elaborar las actas de cada sesión y enviarlas para aprobación y firma de los miembros permanentes que hayan asistido.	Se observó que se lleva a cabo la elaboración de actas del CSICN, acorde con en el formato con código 02-02-FR-01 V1.1, a continuación las siguientes: 1. Acta N° 7, (17 noviembre 2017). 2. Acta N° 1, (15 marzo 2018). 3. Acta N° 2, (16 mayo 2018). Adicional a lo anterior realizó envío a los integrantes del CSICN mediante correos electrónicos para aprobación y posterior firmas
5. Verificar el cumplimiento de las decisiones adoptadas en el seno de las reuniones.	Se observó en las actas antes mencionadas que se registraron los compromisos generados por cada reunión con las fechas de cumplimiento y la dependencia responsable de la actividad. Adicional se evidenció el seguimiento de compromisos generados con anterioridad.
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.	Se observó que la secretará técnica del Comité de Seguridad de la Información y de Continuidad de Negocio, realizó el envió de actas y documentación para el conocimiento de los integrantes del comité para su revisión, comentarios y aprobación; con lo anterior y para verificación la OCI tomó como referencia a los correos electrónicos enviados en las fechas (mar 17/04/2018 y mié 25/07/2018), donde se da cumplimento a las funciones de la Secretaria del Comité SICN.

Funciones del Secretario Técnico del CSICN	Situación Evidenciada
7. Las demás que le sean asignadas por el Comité.	No se evidenciaron para el periodo evaluado.

Fuente: Elaboración propia Resolución 2806 de 2015 – Actas de Comité Sesiones del CSICN noviembre 2017 – junio 2018

5.1.3 Documentación Verificada.

5.1.3.1 Documentos Aprobados por el Comité Seguridad de la Información y Continuidad del Negocio.

Situación Evidenciada:

De la información suministrada por parte de la Gerencia de Tecnología a través de memorando interno cordis 2018IE10417 del 13 de julio de 2018 a la OCI, se observó que en el archivo *"UAECD_ComiteSI&CN_20180516"* informó la documentación para revisión y aprobación por parte de los integrantes del comité de SICN, los siguientes: *"Declaración de aplicabilidad, Plan de trabajo para implementación de controles ISO 27001, Metodología para Gestión de Riesgos en el marco de seguridad de la información, Procedimiento Gestión de Riesgos sobre los activos en el Marco de la Seguridad de la Información, Formato Matriz de Riesgos de Seguridad de la Información"*, Vea imagen N°1 documentos a revisados y aprobados por parte del CSICN.

Imagen N° 1 Documentación para revisión y aprobación CSICN

Verificación de Documentación a Revisar / Aprobar por el CSICN				
Documentos	Revisado	Aprobado	Ejemplo (Intranet, Isodoc, etc)	Link
Declaración de aplicabilidad	x	x	Intranet	http://intranet.catastrobogota.gov.co/?q=es/node/2385
Plan de trabajo para implementación de controles ISO 27001	X	X	Se va a publicar dentro del Plan de trabajo para seguridad y privacidad de la información	
Metodología para Gestión de Riesgos en el marco de seguridad de la información	x	x	En proceso de publicaicón en el SGI	http://sgi.catastrobogota.gov.co/catastrodistritalNew/isodocNew/inicio.nsf?OpendataBase
Procedimiento Gestión de Riesgos Sobre los activos en el Marco de la Seguridad de la Información	x	x	En proceso de publicaicón en el SGI	http://sgi.catastrobogota.gov.co/catastrodistritalNew/isodocNew/inicio.nsf?OpendataBase
Formato Matriz de Riesgos de Seguridad de la Información	x	x	En proceso de publicaicón en el SGI	http://sgi.catastrobogota.gov.co/catastrodistritalNew/isodocNew/inicio.nsf?OpendataBase

Fuente: Correo electrónico suministrado por la Oficial de Seguridad - Documentación aprobada CSICN.

5.1.3.2 Documento Técnico Manual de subsistema de gestión de seguridad y privacidad de la información.

Situación Evidenciada:

Se observó que el documento Técnico Manual de subsistema de gestión de seguridad y privacidad de la información en mención, reposa en el aplicativo ISODOC del SGI con código 02-02-DT-01-V3, en la ruta: http://sgi.catastrobogota.gov.co/catastrodistritalNew/isodocNew/inicio.nsf acorde con lo informado a través del memorando interno cordis 2018IE10417 del 13 de julio de 2018 numeral 15, el Objetivo del documento "*define para la Unidad, las premisas y principios de seguridad de la información, establece los roles y responsabilidades y estructura documental para el Subsistema de Gestión de Seguridad de la Información – SGSI...*"

5.1.3.3 Documento Técnico – Plan de Continuidad del negocio

Situación Evidenciada:

Se verificó el documento técnico Plan de Continuidad del negocio, se evidenció publicado en la intranet de la Unidad en la ruta: http://intranet.catastrobogota.gov.co/sites/default/files/plan-continuidad-uaecd-24-05-2018.pdf, en este documento se describen los planes de Continuidad de los procesos críticos de la Unidad conformada por los equipos de (Manejo de Crisis, Apoyo Operativo, Gerenciales y Equipos Funcionales), donde su responsabilidad es la de atender oportunamente cualquier evento de interrupción, asegurando el restablecimiento de los mismos. Acorde con lo establecido en la Resolución 2806 de 2015 Articulo 3 literal 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*".

Adicional a lo anterior se verificó en la ruta \\fileserver\TI\37_CI_CN se tienen publicados los documentos de Continuidad del Negocio por proceso los siguientes documentos: "*bcp-actuaciones-administrativas-judiciales-ver-18-11-2016, bcp-actualizacion-juridica-ver-18-11-2016, bcp-atencion-reque-geografica-ver-18-11-2016, bcp-atencion-usuario-ver-18-11-2016, bcp-bienestar-ver-18-11-2016 observ sst 06 12 2016, bcp-bienestar-ver-18-11-2016, bcp-comunicaciones-ver-18-11-2016, bcp-gestion - presupuestal-ver-21-11-2016..., informe-drp- 05-05-2017, informe-drp- 21-10-2017*"

Recomendación:

Actualizar periódicamente el cuadro de constancia de aceptación y conocimiento del contenido del plan de continuidad *"FIRMA DE ACEPTACIÓN DEL PLAN DE CONTINUIDAD"* de todos los procesos críticos, ya que contienen nombres de funcionarios que ya no laboraron para la entidad. Se evidenció que en el proceso de *"GESTION DE SERVICIOS DE INFRAESTRUCTURA TECNOLOGICA"* al Gerente de Tecnología nombrado en ese entonces.

5.1.4 Matriz de Riesgos Seguridad de la Información y Continuidad del Negocio

Situación evidenciada:

De los documento enviados por la Gerencia de Tecnología, a través de memorando interno cordis 2018IE10417 del 13 de julio de 2018 *"Seguimiento PMR Riesgos _Seguridad de la información_Junio"* *"Segumiento PMR Riesgos_Continuidad_Junio"* se identificaron los siguientes riesgos asociados a los Subprocesos:–SICN

Los riesgos asociados al Subproceso de Seguridad de la Información, se encontraron distribuidos en la zona residual moderada (2) y baja (1). Así mismo, se definieron acciones para cada riesgo, adicional en el período objeto de verificación no se observó la materialización de eventos de riesgo. Vea tabla N° 3 Riesgos Seguridad de la Información.

Tabla N° 3. Riesgos Asociados a los Subprocesos – Seguridad de la información

Procedimiento	Riesgo	Zona de Riesgo	Acciones a Realizar	Nombre y Descripción del Control
Seguridad de la Información	No activación de la revisión del inventario de activos por proceso después de presentarse una situación que obligue la actualización	Moderado	Realizar revisión del inventario de activos por proceso de manera General con el apoyo de los líderes que sean asignados por cada dependencia por los dueños de proceso	Revisión periódica por parte del oficial de seguridad de los inventarios de activos de información, relacionados para cada uno de los procesos de la Unidad y comunicar los resultados de su revisión al propietario del activo o responsable de cada proceso para que se establezcan las acciones a que haya lugar
	Posible identificación incompleta de las actividades requeridas a incluir en el plan de trabajo	Moderado	Analizar incidentes de seguridad que se hayan presentado para determinar la efectividad de los planes manejo	Documentar planes de manejo específicos de acuerdo con la clasificación del incidente.

Procedimiento	Riesgo	Zona de Riesgo	Acciones a Realizar	Nombre y Descripción del Control
	Posible ausencia en la aplicación de recomendaciones realizadas por Gestión Documental, Seguridad de la Información y Jurídica requeridas para ser incorporadas sobre el inventario de activos por proceso.	Bajo	No se registran en gestión Integral del Riesgo	Ajuste del inventario de activos por parte del equipo revisor y aprobación en segunda instancia por el dueño del proceso

Fuente: Elaboración propia Mapas de Riesgos suministrada por la GT - GT_MapaRiesgosPSSTI_2018_V1.0.xlsx

Los riesgos asociados al Subproceso de Continuidad del Negocio. Se encontraron distribuidos en la zona residual Alta (3) moderada (2) y bajo (4). Así mismo, se definieron acciones para cada Riesgo, adicional en el período objeto de verificación no se observó la materialización de eventos de riesgo como se muestra a continuación tabla N° 4 Riesgos Asociados al subprocesos Continuidad del Negocio.

Tabla N° 4. Riesgos Asociados a los Subprocesos - CN

Procedimiento	Riesgo	Zona de Riesgo	Acciones a Realizar	Nombre y Descripción del Control
Continuidad del Negocio	Posible incumplimiento a la metodología de riesgos, al elaborar el mapa de riesgos	Bajo	N/A	Revisión de mapa de riesgos de acuerdo a la metodología
	Posibles errores y/o temas no desarrollados de importancia, en el informe de riesgos elaborado	Bajo	N/A	Revisión informe de riesgos
	Posible ausencia de compromiso por parte de las directivas de la Unidad para definir, implantar y ejecutar planes de continuidad.	Moderado	1. Se apropió presupuesto a través de los cdps 5 y 6 cuyos valores fueron respectivamente $49'958.416 y 378'668.000 2. Se elaboro el proyecto y se materializo a través de un proceso de Concurso de méritos, adjudicándose a traves de una consultoría cuyo la cual se inicio el 8	Contar con un Subsistema de Gestión de Continuidad del Negocio - SGCN

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

INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO

Procedimiento	Riesgo	Zona de Riesgo	Acciones a Realizar	Nombre y Descripción del Control
			de Marzo	
	Posible ejecución o respuesta inadecuada del plan de continuidad en un evento real	Alto	Se inicio la revisión de cada uno de los procesos y subprocesos de la cadena de valor de la UAECD	1. Actualización de los planes BCP y PAO.
	Posible elaboración errónea del BIA y el RA	Alto	Se inicio la elaboración de la metodología de Análisis de Impacto al Negocio y la metodología al Análisis de riesgos	Elaborar cuestionarios de preguntas exactas y obtener las respuestas oportunamente, para garantizar un adecuado análisis de impacto del negocio y análisis de riesgos
	Posible decisión inadecuada durante la verificación de la aprobación de la estrategia BCP y DRP	Alto	Se inicio la revisión de cada uno de los procesos y subprocesos de la cadena de valor de la UAECD	Aprobación estrategias BCP y DRP
	Posible cubrimiento insuficiente de plan de continuidad frente los servicios que presta la Unidad	Bajo		Validar que el análisis de impacto involucre todos los procesos y subprocesos de la Unidad
	Posible realización de pruebas insuficientes y/o inadecuadas del plan de continuidad	Bajo		1. Identificar y acordar el número adecuado de pruebas en el periodo. 2. Planear las pruebas en periodos de tiempo de poca disponibilidad. Garantizar la definición adecuada para la ejecución de los ejercicios y pruebas de acuerdo a los planes de continuidad del negocio establecidos en la Unidad, teniendo en cuenta la capacidad de los recursos (humano, tecnológico e infraestructura física) y las criticidades de los procesos.

Procedimiento	Riesgo	Zona de Riesgo	Acciones a Realizar	Nombre y Descripción del Control
	Posible plan de ejercicios y pruebas mal diseñado y desarrollado	Moderado	Se inicio la revisión de cada uno de los procesos y subprocesos de la cadena de valor de la UAECD	1. Planear las pruebas en periodos de tiempo de poca disponibilidad. 2. Contar con pruebas divulgadas y acordadas con la alta gerencia.

Fuente: Elaboración propia OCI con base a la información suministrada en archivo - GT_MapaRiesgosPSSTI_2018_V1.0.xlsx

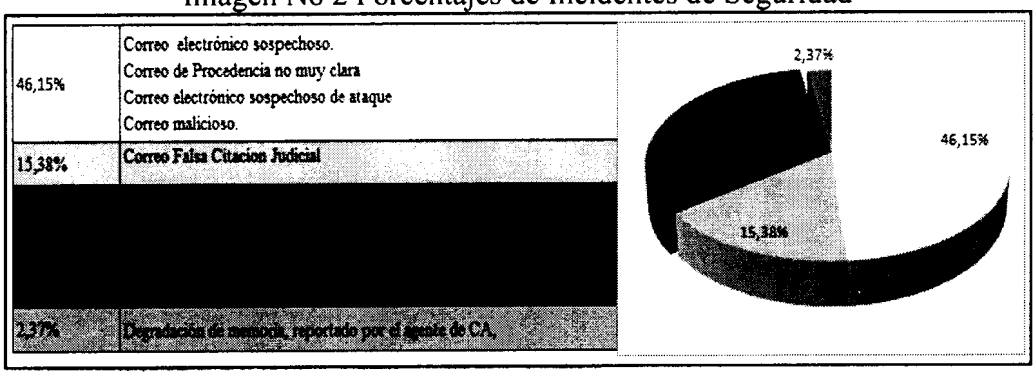
5.1.5 Seguimiento Incidentes de Seguridad

Situación Evidenciada:

Se Observó en el período evaluado el registró de 13 incidentes de seguridad en la mesa de ayuda (CA) de la UAECD , catalogados de la siguiente manera: el 46.15% de 6 ítems, corresponden a correos externos enviados a funcionarios de la unidad (correos electrónicos informados como sospechosos de ataque, de procedencia no muy clara, y maliciosos), el 15.38% (2) provienen de correos externos (falsa citación judicial), el 30.77% (4 ítems) presentaron accesos a sitios no autorizados (minería cryptomoneda), adicional utilizaron aplicaciones para eludir el proxy de la Unidad, mientras que el 2.37% por degradación de memoria.

Lo anterior acorde con lo informado en el acta N° 1 de marzo 15 de 2018 al CSICN y como compromiso por parte de la Gerencia de Tecnología; tomó las respectivas medidas para cada caso, entre otras él envió de memorando a la oficina de Control Interno Disciplinario. *"Informando los usuarios que se detectaron haciendo mal uso de Internet"* a continuación vea imagen N° 2. Porcentajes de Incidentes de Seguridad en la vigencia en mención.

Imagen No 2 Porcentajes de Incidentes de Seguridad



Fuente: Elaboración Propia OCI - Archivo Incidentes de Seguridad

Cabe aclarar: que la siguiente actividad realizada por la OCI, se encuentra fuera del periodo evaluado y es conveniente informarla a la Gerencia de Tecnología y tomen las acciones pertinentes para con la recepción de correos masivos comerciales enviados a la entidad, donde se tomó muestra del 1.03% (7 usuarios) de 678 equipos que conforman la unidad, (vea tabla No 5 correos institucionales) se observó la recepción de correos externos con publicidad comercial masiva así: *"Chevrolet La marca màs vendida cambiò. Descùbralo!!!"*, *"Presentaciòn Equinox, una camioneta hecha a su medida Cero por ciento interés"*, *"AGENDA CHEVROLET SAN JORGE"*, *"Promoción Emermedica"*, *"¿Te gustaría ser distribuidor? Contáctenos..."* dado lo anterior y acorde con lo establecido en el *"PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"*, la OCI procedió al registro de lo acontecido en el aplicativo de mesa de servició - Ca service manager (SOL0148465-18 del 07/27/2018). donde fue catalogado como *"Incidente Menor por cuanto no afecta la ejecución normal de los procesos"*, adicional se estableció el siguiente plan de trabajo:

1. *"Revisar con la SIT las reglas de filtrado para los dominios reportados: Se hace claridad que el dominio ya había sido reportado en varias ocasiones y se habían creado las reglas de filtrado, no obstante ante la reincidencia de los correos se volverá a revisar la regla creada.*

2. *Se revisará la necesidad de escalar el incidente a otra instancia*

3. *Se realizarán socializaciones a la entidad con el fin de contextualizar acerca de los correos clasificados como contenido abusivo."*

Tabla N° 5 Correos de la UAECD donde llegó Información Comercial

Correo usuarios	Dependencia UAECD
Jlinares@catastrobogota.gov.co	Dirección
dvargas@catastrobogota.gov.co emrodriguez@catastrobogota.gov.co	Oficina Asesora Planeación y Aseguramiento de procesos
jnavas@catastrobogota.gov.co jberbeo@catastrobogota.gov.co jroncancio@catastrobogota.gov.co dbaquero@catastrobogota.gov.co	Oficina de Control Interno

Fuente: Elaboración propia OCI correo institucional UAECD

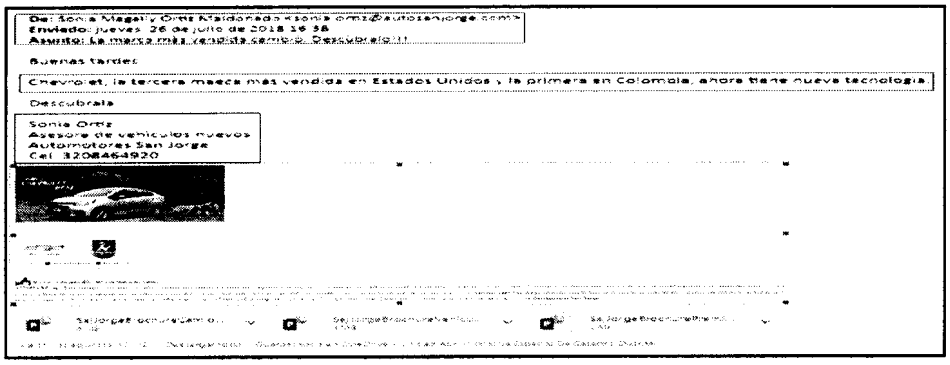
Adicional se evidenció: Para el usuario emrodriguez@catastrobogota.gov.co de OAPAP. Le fue enviado a nombre propio publicidad comercial de la entidad externa *"Artecmac Diseños en Madera SAS"* invitandole

a ser distribuidor de productos que ofrecen, adicional en este correo se muestra un link para actualización de datos (Posible Phising[1]).

A continuación se presentan los casos 1 y 2 antes mencionados así:

Caso N° 1 Correos externos con publicidad comercial de "*Chevrolet*" enviados a cada uno de los funcionarios y contratistas de la unidad.

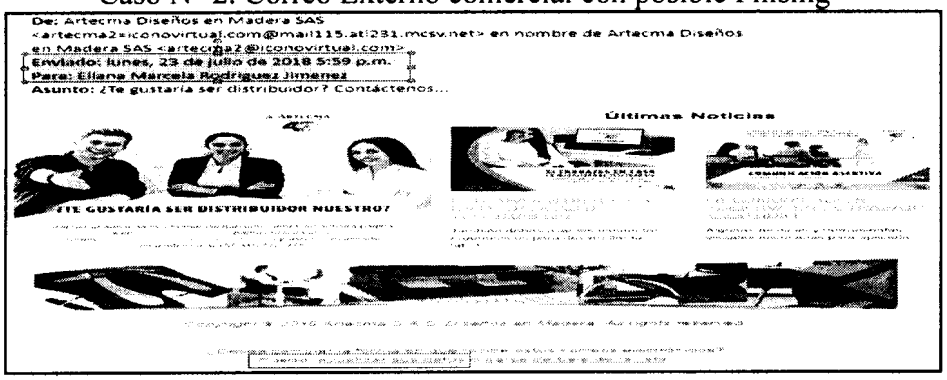
Caso No 1 Correo Externo con Publicidad comercial



Fuente: Correo remitido por funcionarios UAECD

Caso N° 2 Correo dirigido con publicidad por parte de entidad externa *"Artecmac Diseños en Madera SAS"* a funcionaria y a nombre propio.

Caso N° 2. Correo Externo comercial con posible Phising



Fuente: Correo remitido por funcionaria- OAPAP

[1] ***Phishing***, conocido como **suplantación de identidad** o simplemente **suplantador**, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.[1]

Recomendaciones:

- Solicitar a todas las dependencias de la Unidad (funcionarios, contratistas etc.) registren en mesa de servicios de la Unidad, la recepción de correos con procedencias dudosa entre ellos: (correos extraños, correos con información comercial, correos enviados de entidades financieras, correos externos con adjuntos y direccionamientos a formularios de diligenciamiento con datos personales) con el fin de ser analizados, catalogados y solucionados por el grupo de apoyo de Seguridad de la Información.
- Monitoreo constante de los correos entrantes a la unidad con el fin de identificar Malware[2], Phising virus troyanos.
- Ofrecer al interior de la UAECD charlas de concientización en Seguridad de la Información.
- Dar a conocer a la Unidad que se pueden realizar denuncias de incidentes informáticos al equipo C-SIRT de la policía nacional en el link siguiente: https://cc-csirt.policia.gov.co/

5.1.6 Seguimiento de Incidentes registrados en Mesa de ayuda

Se observó en el listado enviado por la Gerencia de Tecnología, a través de memorando interno Cordis N° 2018IE10417 del 13 de julio de 2018 enviado a la OCI, se evidenció en el el aplicativo de mesa de ayuda *"CA Service Desk Manager"* Se registraron los incidentes de Seguridad de la Información, adicional se verificó en el aplicativo y se encuentran cerrados. Vea Tabla N° 6 Incidentes de seguridad

Tabla N° 6 Listado de Incidentes de Seguridad Información

Incidente	Fecha	Observación OCI
SOL0139082-18	09/03/2018 12:01	Se evidenciaron cerrados en el aplicativo CA Service Desk Manager
SOL0139049-18	09/03/2018 10:14	
SOL0143733-18	17/05/2018 16:41	
SOL0139331-18	13/03/2018 16:02	
SOL0146626-18	28/06/2018 07:39	Se evidenciaron cerrados en el aplicativo CA Service Desk Manager, se observo que los incidentes presentaos fueron reportados en su momento por los usuarios adjuntando soportes.
SOL0139092-18	09/03/2018 14:06	
SOL0137204-18	18/02/2018 21:56	
SOL0132414-17	14/12/2017 10:04	
SOL0132380-17	14/12/2017 07:21	
SOL0132372-17	13/12/2017 17:25	
SOL0132367-17	13/12/2017 16:58	
SOL0132365-17	13/12/2017 16:40	
SOL0132364-17	03/12/2017 16:38	

Fuente: elaboración propia OCI – Archivo Excel Incidentes de Seguridad

[2]Malware es la abreviatura de "*Malicious software*", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers. Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc.... https://www.infospyware.com/articulos/que-son-los-malwares/

Recomendaciones:

Socializar al interior de la Unidad la importancia de reportar cualquier incidente de seguridad de la Información, adicional sea reportado en el aplicativo "CA Service Desk Manager" con el fin que esta información sea analizada y se evalué su grado de complejidad.

5.1.7 Seguimiento acciones de mejora - Seguridad de la Información.

Situación Evidenciada:

Se observó que las acciones de mejora PDA-2017-125 y PDA-2018-240 se encuentran en proceso de implementación, gestionadas dentro de los términos programados. Vea a continuación Tabla N° 7 Acciones de Mejora.

Tabla N° 7 Acciones de Mejora

Acción	Descripción de ISODOC	Observación OCI
PDA-2017-125 En proceso	Se crea esta acción para dar continuidad a la PDA-2016-749, Se presentó incumplimiento de la meta establecida del indicador "Cumplimiento en la instrumentalización de controles de seguridad de la información" para los siguientes periodos: a. Primer semestre del año 2016, meta del 90%, con resultado de 57,14%. b. Segundo semestre del año 2016, meta del 90%, con resultado de 50,00%. c. Primer trimestre del año 2017, meta del 30%, con resultado de 18,39%. (El término instrumentalización hace referencia a las actividades de Elaborar/actualizar, presentar, revisar [1ª. Instancia], ajustar, revisar [2ª instancia] ajustar, verificar, aprobar, socializar y solicitar la publicación de los entregables definidos para cada uno de los controles de seguridad de la información definidos)	Se establecieron 9 acciones de las 8 se evidenciaron en el ISODOC – SGI cumplidas 100%, la ACT-2018-784 / En Proceso "Seguimiento indicador "Cumplimiento en la instrumentalización de controles de seguridad de la información" no ha dado inicio, no se evidenció avance 0% Fechas de Finalización, primera fecha 31/07/2018 Segunda fecha se amplió para el 31/10/2018. Promedio actual 88.89%.
PDA-2018-240 / En Proceso	Instrumentalizar la política para dispositivos móviles que se encuentra incluida en el Documento técnico manual de políticas detalladas de seguridad y privacidad de la información publicada en el Sistema de Gestión Integral - SGI.	Se crearon 2 actividades, 1 se evidenció en el ISODOC – SGI cumplidas 100%, la ACT-2018-638 / En Proceso "Programar el desarrollo de jornadas de sensibilización acerca de los controles para el uso de dispositivos móviles que acceden a la información de la Unidad." , no ha dado inicio, avance 0%. Fechas de Finalización: primera fecha 31/05/2018 Segunda fecha se amplió para el 31/08/2018Promedio actual 50%.

Fuente: aplicativo ISODOC.

Recomendación: Realizar cargues de información en las PDA con el fin de dar avance a la actividad las cuales vencen en agosto y octubre

5.1.8 Seguimiento a los acuerdos de confidencialidad de personal

Se observó que los pasantes vinculados a la entidad entre el 01 de noviembre de 2017 al 30 de junio de 2018, son procedentes de la Universidad de los Andes y Universidad Distrital Francisco José de Caldas, y autorizados por la Subgerencia de Recursos Humanos quienes apoyaron las actividades programadas por la Oficina de Control Interno y Gerencia de Gestión Corporativa, adicional se evidenció firmado el formato *"Compromiso de Confidencialidad Para El Manejo Y Buen Uso dela Información y la Tecnología de la Unidad Administrativa Especial De Catastro Distrital – UAECD Estudiantes en calidad de practicantes, pasantes, tesistas en proyecto de grado y judicantes"*, vea imagen N° 3 pasantes autorizados por SRH.

Imagen N° 3 pasantes vigencia 2017 - 2018

UNIDAD ADMINISTRATIVA ESPECIAL DE CATASTRO DISTRITAL
GERENCIA DE GESTION CORPORATIVA
Subgerencia de Recursos Humanos

Informe de pasantes entre el 01 de octubre de 2017 al 30 de junio de 2018

N°	Nombre del pasante	Identificación	Institución Educativa	Dependencia	Fecha inicio	Fecha finalización	Actividades Programadas
1	Sergio Alejandro Quiroga Ospina	1010234890	Universidad de los Andes	Oficina de Control Interno	05/06/2018	03/08/2018	Revisión de los modelos econométricos utilizados en la actualización Catastral.
2	Daniela Hernández Morales	1'030.616.348	Universidad Distrital Francisco José de Caldas	Gerencia de Gestión Corporativa	21/05/2018	20/11/2018	Apoyo al Plan Institucional de Gestión Ambiental PIGA y Componentes Afines
3	Iván Ronaldo Ray Gómez Aragón	1'000.116.623	Universidad Distrital Francisco José de Caldas	Gerencia de Gestión Corporativa	29/05/2018	28/11/2018	Apoyo al Plan Institucional de Gestión Ambiental PIGA y Componentes Afines

Nellyret Moreno Ramos
Profesional Especializada
Subgerencia de Recursos Humanos

Fuente: Archivo enviado por Subgerencia de Recursos Humanos

5.1.9 Seguimiento Contrato 191 de 2018 Consorcio Mnemo SGSI

5.1.10.1. Acta de inició Consorcio Mnemo SGSI

Situación evidenciada.

Se observó la información sumistrada por la Gerencia de Tecnología y mediante Cordis N° 2018IE10417 del 13 de julio de 2018 enviado a la OCI, que el "*ACTA DE INICIO CONTRATO N° 191-2018*" Contratista "*Consorcio Mnemo SGSI*", inició en marzo 8 y finaliza el 7 de noviembre de 2018 respectivamente, valor del contrato $427.626,416, adicional en el acta se encontró firmada por el contratista y funcionarios de la Unidad,

5.1.10.2. Documentos entregados por parte del Contratista

Situación evidenciada.

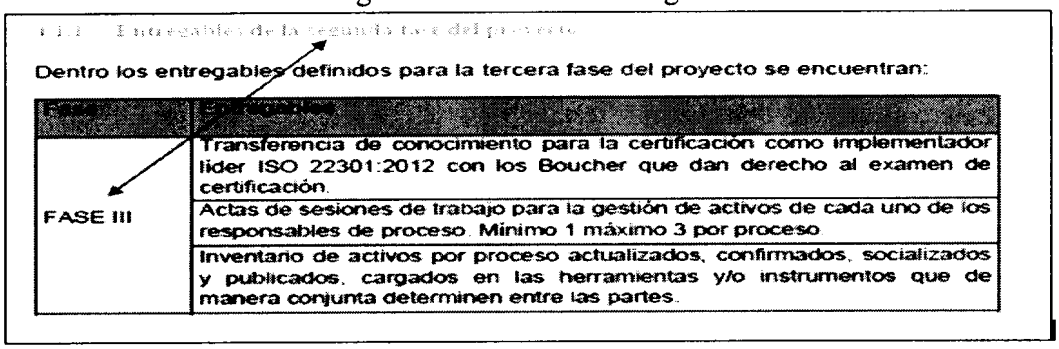
Como parte de las actividades desarrolladas dentro del contrato número 191 de 2018 *"Consorcio Mnemo SGSI"*, se observó que mediante memorando enviado por la Gerencia de Tecnología Cordis 2018IE10417 del 13 de julio de 2018, envió a la OCI, los siguientes documentos:

1. Informe de Seguimiento mes de marzo fase I.
2. Informe de Seguimiento mes de abril fase II.
3. Informe de Seguimiento mes de mayo fase III.

No obstante se observó en el "*Informe de Seguimiento mes de mayo fase III*", el literal 4.1.1 hace alusión a la segunda fase del proyecto, siendo de la fase III, adicional se observó que el encabezado corresponde al mes de abril.

Recomendación: Solicitar al contratista *"Consorcio Mnemo SGSI"* se revise el contenido del informe de seguimiento mayo 2018, ya que difiere la información del literal "*4.1.1 Entregables de la segunda fase*", adicional se sugiere se incluyan recomendaciones y conclusiones por cada informe entregado.

Imagen No 4 literal de entregables



Dentro los entregables definidos para la tercera fase del proyecto se encuentran:

FASE III	Transferencia de conocimiento para la certificación como implementador lider ISO 22301:2012 con los Boucher que dan derecho al examen de certificación.
	Actas de sesiones de trabajo para la gestión de activos de cada uno de los responsables de proceso. Mínimo 1 máximo 3 por proceso
	Inventario de activos por proceso actualizados, confirmados, socializados y publicados, cargados en las herramientas y/o instrumentos que de manera conjunta determinen entre las partes.

Fuente: Informe de Seguimiento Mes de Mayo 2018 – Contrato 193-2018 "*Consorcio Mnemo SGSI*",

5.1.10.3. Actividad cursos Implementador ISO22301:2012.

Situación evidenciada.

Entre los entregables por parte del contratista *"Consorcio Mnemo SGSI"*, es la de capacitar a diez funcionarios de la Unidad como implementadores líderes ISO 22301:2012, donde se evidenció en el *"informe de seguimiento del proyecto del mes de abril 2018"* que 9 de los 10 funcionarios escogidos por las dependencias, aprobaron el examen y fueron certificados como *"Líder Implementador ISO 22301:2012"*, realizado entre el 21 y el 30 de mayo de 2018, cumpliendo satisfactoriamente los requisitos de formación exigidos por el Registro Europeo de Auditores Certificados - ERCA. Sin embargo uno de ellos no aprobó el examen sin ser certificado, a lo anterior la entidad -ERCA permite presentar nuevamente el examen, con la condición que este sea realizado en la vigencia del año siguiente y sea certificado el funcionario. Vea a continuación imagen No 5 la descripción de los resultados:

Imagen No 5 Descripción de los resultados ISO 22301:2012.

Item	Apellidos	Nombre	Cédula	Experiencia	Talleres y Asistencia	Examen	RESULTADO Final
1	Barrera Barrera	Pedro Nel	19.294.575	No	Aprobado	Aprobado	Aprobado
2	Berbeo Rodríguez	José Manuel	4.151.627	No	Aprobado	Aprobado	Aprobado
3	Bolívar Ospina	Manuel Tiberio	79.152.906	No	Aprobado	Aprobado	Aprobado
4	Español Morales	Edgar Estevens	79.721.436	No	Aprobado	Aprobado	Aprobado
5	Navarro Hernández	Sergio Andrés	1024.495.451	No	Aprobado	Aprobado	Aprobado
6	Numpaque Fraile	Pedro Alfonso	79.374.364	No	Aprobado	Aprobado	Aprobado
7	Sánchez Orjuela	Jhon Jairo	79.897.775	No	Aprobado	Aprobado	Aprobado
8	Torres Aguilar	Claudia Patricia	51.910.591	No	Aprobado	Aprobado	Aprobado
9	Torres Malaver	Orlando	19.286.883	No	Aprobado	Aprobado	Aprobado
10	Rincón Rueda	Javier Ricardo	80.410.647	No	Aprobado	No Aprobado	No Aprobado

Fuente: Informe de Seguimiento Mes de Mayo 2018 – Contrato 193-2018 *"Consorcio Mnemo SGSI"*,

5.1.10.4 Documento Plan de Trabajo.

Situación Evidenciada:

Se observó en cronograma de actividades Catastro – 3 enviado por la oficial de Seguridad de la Información el 18 de julio de 2018, donde se presentó el proyecto acordes a la *"Estrategia de Continuidad del Negocio"*, con sus respetivas actividades que iniciaron el 05/07/2018 al 03/10/2018, ver anexo No 1 del informe.

CONCLUSIONES

De acuerdo con el resultado del Seguimiento Comité de Seguridad de la Información y continuidad de Negocio – CSICN, se concluye que la Unidad esta dando cumplimiento a lo establecidos en 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".*

RECOMENDACIONES:

- Mayor participación de los integrantes de comité a reuniones convocadas.
- Realizar monitoreo constante de incidentes de seguridad y riesgos presentados en la Unidad.
- Continuar con el seguimiento del mal uso de Internet y publicación de Ranking al interior de la Unidad.
- Sensibilización a funcionarios en cuanto a reportar incidentes de seguridad en la herramienta de mesa de ayuda
- Seguimiento al contrato 191-2018 Mnemo SGSI, en cuanto a reuniones, compromisos semanales, entregables en todas las fases, oportuno aprovechamiento y aprendizaje que ofrece el contratista, solicitar capacitaciones SICN e infundirlas a los funcionarios de la Unidad.
- Actualización de documentación de Continuidad del Negocio.
- Continuar con el fomento a la cultura de Gestión de Continuidad de Negocio al interior de la Entidad.
- Continuar con el seguimiento y evaluación a la Gestión de Continuidad de Negocio para identificar oportunidades de mejora.

Los resultados de la revisión documental realizada en este informe y las evidencias obtenidas de acuerdo con los criterios definidos, se refieren solo a los documentos examinados y no se hacen extensibles a otros soportes.

Agradezco remitir las observaciones respecto a los resultados del presente informe, antes del próximo 15/08/2018, a los correos jnavas@catastrobogota.gov.co, dbaquero@catastrobogota.gov.co

Cordialmente

JOHNY GENDER NAVAS FLORES
Jefe Oficina de Control Interno

ELABORÓ Y VERIFICÓ.
DANILO FERNANDO BAQUERO GONZALEZ
Contratista Oficina Control Interno.

Revisó: Hederson Agudelo Ortiz
Contratista Oficina Control Interno.

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

INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO

ANEXOS No 1

Cronograma de actividades Catastro – 3

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

PROCESO GESTIÓN INTEGRAL DEL RIESGO: SUBPROCESO GESTIÓN DE CONTINUIDAD DEL NEGOCIO
GERENCIA DE TECNOLOGÍA

PLAN DE TRABAJO - VIGENCIA 2017

Subsistema de Gestión de Continuidad del negocio – SGCN

Elaboró: Jose Abraham Villarraga Rios, Oficial de Continuidad
Revisó: José Luis Arza Vargas, Gerente de Tecnología
Aprobó: Comité de Seguridad y Continuidad
Fecha actualización: 2018-03-12

BOGOTÁ MEJOR PARA TODOS

2018

Item	Actividad	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Responsable
	Etapa Planeación.													
1	Firma del acta de inicio del proyecto													Oficial Continuidad - Consultor
2	Formalización de proyecto													UAECD - Consultor
3	Planeacion													Oficial Continuidad - Consultor
4	Reunion kick Off													Oficial Continuidad - Oficial seguridad - Consultor
5	Socialización del SGI, respecto a los lineamientos planteados en la Unidad													Oficial Continuidad - Oficial seguridad
6	Suministro de la información del SGI asociado al proyecto por parte de la Unidad													Oficial de Continuidad
7	Desarrollar el plan para la dirección de proyecto													Consultor
8	Seguimiento al proyecto													Oficial Continuidad - Oficial seguridad - gerente proye
9	Etapa Ejecución.													
10	Desarrollar informes mensuales de ejecucion de actividades de acuerdo al plan de trabajo acordado con la entidad													Gerente proyecto
11	Reuniones de Seguimiento al proyecto													Oficial Continuidad - Consultor
12	Presentar del estado del proyecto Mayo - Junio - Julio - Srpbre - Nov													Consultor
13	Análisis Tecnico y Financiero de la Herramienta y/o solución para la gestion de SGSI, SGCN y RA													Consultor
14	Revisar las necesidades de la Unidad de Catastro respecto a la herramienta y/o solución para la gestion													Consultor
15	Realizar el análisis de las herramientas y/o soluciones existentes en el mercado que permitan llevar a cabo la gestión del SGSI, SGCN y RA.													Consultor
16	Análisis del impacto del Negocio y Riesgos de Interrupción													Consultor - oficial Continuidad
17	Metodología para el análisis de impacto al negocio (BIA)													Consultor
18	Realizar el análisis de la información recaudada													Consultor
19	Elaborar la metodología para el análisis de impacto al negocio (BIA)													Consultor
20	Metodología para el análisis de riesgos de interrupción (RA)													Consultor
21	Realizar análisis de la información recaudada													Consultor
22	Elaborar la metodología para el análisis de riesgos de interrupción (RA)													Consultor
23	Configurar en la herramienta y/o instrumento determinar el resultado obtenido del análisis de riesgos de interrupción													Consultor
24	Informe con las acciones realizadas en la herramienta y/o instrumentos definidos de manera													Consultor
25	Resultado de análisis del Impacto Financiero													Consultor
26	Realizar entrevistas con los dueños de proceso													Oficial Continuidad - Consultor
27	Realizar el análisis a los distintos procesos y consolidar información													Oficial Continuidad - consultor
28	Producir riesgos de interrupcion													Consultor
	Configurar en la herramienta y/o instrumento determinar el resultado obtenido del análisis de impacto													Consultor
29	Desarrollar las pruebas de los procesos criticos (3)													Consultor - oficial de Continuidad
30	Estrategia de Continuidad del Negocio													Oficial Continuidad - Consultor
31	Identificar escenarios de desastre													Consultor - oficial Continuidad
32	Formular estrategias de continuidad de operaciones													Consultor - oficial de Continuidad
33	Elaborar la estrategia de continuidad del negocio													Consultor
34	Estrategia de recuperación de desastres													Consultor
35	Plantear estrategias para el centro de cómputo													Consultor
36	Elaborar estrategias telecomunicaciones y seguridad													Consultor

Fuente: Archivo suministrado por la Gerencia de Tecnología – SGCN_PlandeTrabajo_2018-03-12

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

INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO

Continúa Cronograma de actividades Catastro – 3

37	Elaborar estrategias para datos	Consultor
38	Elaborar la estrategia de recuperación de desastres	Consultor
39	Planes de continuidad de negocio	Consultor
40	Desarrollar el modelo de gobierno de continuidad de negocio	consultor
41	Elaborar planes de continuidad	Consultor
42	Plan de respuesta a emergencias	Consultor
43	Plan de manejo de crisis	Consultor
44	Plan de continuidad de procesos de negocio de 15 procesos del negocio	Consultor
45	Elaborar el documento con el plan de continuidad del negocio	Consultor
46	Planes de recuperación de desastres (Tecnología)	Consultor
47	Desarrollar el modelo de gobierno de DRP	Consultor
48	Definir los procedimientos técnicos de DRP	Consultor
49	Procedimiento de suministro eléctrico	Consultor
50	Procedimiento de Comunicaciones y Redes	Consultor
51	Prodcedimiento de seguridad perimetra	Consultor
52	Procedimiento de almacenamientos	Consultor
53	Plan de servidores	Consultor
54	Procedimiento de aplicaciones y servicios criticos	Consultor
55	Elaborar el plan de recuperación de desastres	Consultor
56	Presentar el plan de recuperación de desastres	Consultor
57	Solicitar la publicación el plan de recuperación de desastres	Consultor
58	Informe de resultados del ejercicio	Consultor
59	Elaborar el plan del simulacro de 3 procesos criticos	Consultor
60	Revisar y aprobar el plan de simulacro	Consultor
61	Realizar el simulacro	Consultor
62	Elaborar el informe de resultados del ejercicio	Consultor
63	Diagnóstico de Continuidad de Negocio	Consultor
64	Revision de la documentacio respecto a los requisitos de la ISO 22301:2012	Consultor
65	Analizar el nivel de cumplimiento de los requisitos normativos de la ISO 22301:2012	Consultor
66	Elaborar el informe de diagnóstico de continuidad del negocio	Consultor
67	Mapa de ruta Continuidad de negocio	Consultor
68	Realizar el análisis de los resultados obtenidos del diagnóstico y recomendaciones	Consultor
69	Desarrollar un informe de estrategias implementadas	Consultor
70	Restructuración de las estretegias recomendadas	Consultor
71	Definir las actividades requeridas por la entidad en los próximos 3 años (2018, 2019, 2020)	Consultor
72	Elaborar el mapa de ruta con las actividades requeridas para la continuidad del negocio	Consultor
73	Transferencia de conocimiento	Consultor
74	Coordinar el desarrollo de las capacitaciones	Consultor
75	Realizar la capacitaciones de implementadores de ISO 22301:2012 a los 10 funcionarios de la entidad	Consultor
76	Entregar los vouchers para el examen de certificación	consultor
77	Cierre del proyecto	Consultor - oficial de continuidad
78	Entregar las versiones finales de los productos del proyecto	Consultor
79	Presentaction final de los resultados	Consultor - oficial continuidad
80	Firma acta final del proyecto	Consultor - oficial de continuidad

Fuente: Archivo suministrado por la Gerencia de Tecnología – SGCN_PlandeTrabajo_2018-03-12