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 [ ] Auditoría de Gestión [X]

En cumplimiento del Plan Anual de Auditorías de la vigencia 2019 a continuación, se presentan los resultados del Informe citado dirigido a la directora de la UAECD con copia a las áreas o procesos involucrados.

Proceso: Gestión Integral del Riesgo.

Subproceso: Gestión de Seguridad de la Información.

NOMBRE DEL INFORME:

Auditoría de Gestión de Seguridad y Privacidad de la Información.

1. OBJETIVO GENERAL

Verificar el uso y apropiación de los lineamientos definidos para el SGSI en la UAECD.

2. OBJETIVOS ESPECIFICOS

- Determinar la conformidad del Subsistema de Seguridad y Privacidad de la Información de la UAECD con los requisitos establecidos en la norma ISO 27001:2013.

- Verificar la aplicación y apropiación de los lineamientos del SGSI de la UAECD por parte de los servidores públicos.

3. ALCANCE

Verificar y evaluar el cumplimiento de lo establecido a través de los procesos, procedimientos, instructivos, formatos y demás documentos y normatividad aplicable al Subsistema de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Catastro Distrital, de enero a septiembre de 2019, en las áreas de Gerencia de Tecnología, Gerencia Comercial y de Atención al Usuario, Gerencia de Infraestructura de Datos Espaciales, Subgerencia Administrativa y Financiera y, la Subgerencia de Recursos Humanos.

4. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA

- La norma ISO 27001 versión 2013.
- Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, Código: 02-02-DT-02, versión: 5 del 28-02-2019 y versión 6 del 23-10-2019.
- Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, código 02-02-DT-01, versión 4 del 24-12-2018.
- Declaración de Aplicabilidad Seguridad de la Información, versión 2 del 26-02-2018.
- Procedimiento Gestión de Accesos, código: 13-02-PR-04, versión: 4 del 05-07-2018.
- Procedimiento Gestión de Incidentes de Seguridad de la Información, código 02-02-PR-01, versión 5, fecha 05/09/2019
- Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06, versión 1 del 03-09-2019,
- Modelo de Seguridad de la Información, versión 1 del 08/04/2016.
- La demás normatividad externa e interna aplicable al tema de la auditoría.

5. METODOLOGÍA

La auditoría se realizó dentro del marco de las normas de auditoría internacionales, las cuales incluyeron: planeación, ejecución, generación y comunicación del informe con las conclusiones y recomendaciones que permitirán contribuir al mejoramiento del Sistema de Control Interno.

Para el desarrollo de la auditoría, durante el mes de julio de 2019, la Oficina de Control Interno, realizó convocatoria a los funcionarios que están certificados como auditores internos en la norma ISO 27001:2013, con el fin de aprovechar el recurso humano formado por la entidad. Así, luego de 2 reuniones para informar el tema de la auditoría y solicitar la participación de los auditores, se contó con la participación de cuatro -4- funcionarios: Angela Indira Suarez de IDECA, Diana Hasbleidy Calderón y Sandra Lucía Rincon de la Gerencia de Información Catastral y, Carlos Hernan Tovar de la Gerencia de Tecnología.

Se realizaron siete reuniones como preparación para la auditoría, de julio a octubre de 2019, con el apoyo del grupo de seguridad de la información de la Gerencia de Tecnología, en temas como: Norma ISO 27001:2013, perfil del auditor, recomendaciones para el desarrollo de la auditoría, estructuración del SGSI en la Unidad, entre otros.

Para el desarrollo de la auditoría se tomaron como base principal lo dispuesto en el "Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información", en cuanto a que en él se establecen los lineamientos principales (alcance, objetivos, principios, responsabilidades) de las 12 políticas de seguridad y privacidad de la información de la UAECD y los procedimientos relacionados con las mismas.

Se elaboraron y aplicaron 39 listas de verificación para usuarios, con el fin de comprobar el uso y apropiación de los lineamientos para la gestión de incidentes de seguridad de la información, áreas

seguras, activos de información, escritorio y pantalla limpios, transferencia de información y aspectos relacionados con la gestión de continuidad del negocio.

Así mismo, se elaboraron y aplicaron listas de verificación específicas en temas de áreas seguras, transferencia de información a terceros y a la Oficial de Seguridad.

6. PRESENTACIÓN DE RESULTADOS

Para la presentación de resultados se tomó como base la Declaración de Aplicabilidad de la UAECD, V.2., del 26/02/2018, que es el documento que lista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 versión 2013 (un conjunto de 114 controles agrupados en 35 objetivos de control), sobre la cual se relacionan los objetivos de control y los controles que se encuentran implementados en la Unidad y los que se descartaron, debidamente justificados.

Nota: Para el presente informe se aclara que la sigla "S.E." se traduce como situación evidenciada.

6.1. Revisión Declaración de Aplicabilidad.

La Declaración de Aplicabilidad Seguridad de la Información, versión 2.0 del 26/02/2019 de la UAECD, de acuerdo con lo indicado en su Introducción, "*Este documento da un panorama amplio de lo que está haciendo la Entidad para proteger su información, ya que identifica, organiza y registra las medidas de seguridad propuestas por la citada norma (...)*" relaciona los controles correspondientes al Anexo A de la norma NTC ISO 27001:2013.

A continuación, se muestra el consolidado de la revisión efectuada por la OCI, a la implementación de los dominios (14), objetivos (35) y controles de seguridad (114) indicados en la norma ISO 27001:2013, y el control descrito en la Guía No. 8 del Mintic "Controles de Seguridad y Privacidad de la Información". Ver **Anexo No. 1, CONSOLIDADO DE LA REVISIÓN EFECTUADA POR LA OCI, A LA IMPLEMENTACIÓN DE LOS DOMINIOS (14), OBJETIVOS (35) Y CONTROLES DE SEGURIDAD (114) INDICADOS EN LA NORMA ISO 27001:2013**.

Nota: Los dominios, objetivos o controles que no están relacionados en el anexo, fueron revisados en su totalidad, sin embargo, no presentan recomendaciones, oportunidades de mejora o acciones correctivas.

6.1.1. Política de la Seguridad de la Información (Dominio A.5 NTC-ISO/IEC 27001:2013)

A.5.1.1 Políticas para la seguridad de la información.

Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

S.E. Se observó que el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, Código: 02-02-DT-02, versión 6 del 23-10-2019, contiene 12 políticas así: control de acceso, escritorio y pantalla limpios, tratamiento de datos personales, instalación y uso de software, uso aceptable, transferencia de información, copias de respaldo y recuperación, dispositivos móviles, relación con proveedores en la etapa precontractual y contratistas, gestión de la seguridad de las redes, desarrollo seguro y política para el uso de controles criptográficos.

Recomendación: Se deben modificar los siguientes ítems en el Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, código 02-02-DT-01, así:

- *2.5.3 Localizaciones físicas incluidas*, actualizar la dirección del archivo central y la empresa contratada.
- *2.5.5. Sistemas de información incluidos en el SGSI*, actualizar, falta avalúos comerciales, FOCA y Captura en Terreno.
- *2.8. El plazo para la implementación de este manual es diciembre de 2018*, modificar la fecha de acuerdo con la proyección para la implementación que tenga actualmente la UAECD.

A.5.1.2 Revisión de las políticas para seguridad de la información

Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

S.E. Se observó que en el Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, numeral 2.4.1 Políticas de la seguridad de la información, se indica: *b) La Unidad deberá **revisar las políticas para seguridad de la información a intervalos planificados** de acuerdo con lo exigido en los requerimientos regulatorios que le aplican a su naturaleza o cuando ocurran cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas* y *c) Las políticas definidas para cada dominio de control y que se encuentran en los numerales siguientes deberán tener un propietario que adquiera la responsabilidad de desarrollar, revisar, evaluar y apropiar las políticas con el apoyo del oficial de seguridad de la información acorde al numeral 2.6 Roles y responsabilidades del SGSI. La **revisión** deberá incluir la valoración de las oportunidades de mejora de las políticas de la Unidad y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno organizacional, las circunstancias de la Unidad, las condiciones legales o el ambiente técnico*.

S.E. El documento de políticas detalladas ha sido modificado en 2 ocasiones durante la vigencia 2019.

S.E. En la Declaración de Aplicabilidad, se indica que se cuenta con el Procedimiento Revisión por la Dirección Al SGI, código 14-01-PR-10, V.2, del 30/11/2018, sin embargo, en dicho procedimiento no se establece una periodicidad para la revisión de las políticas del Sistema Integral de Gestión -SIG, que incluye el Subsistema de Seguridad y Privacidad de la Información.

Hallazgo
(OM) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció que las modificaciones al documento de políticas detalladas del SGSI no han estado relacionadas con el procedimiento de Revisión por la Dirección, teniendo en cuenta que en las actas del Comité Institucional de Gestión y Desempeño 2019, se observó una presentación del Subsistema en el mes de julio de 2019, pero no se evidenció la revisión de las políticas de seguridad de la información. Así mismo, no se observó en ningún documento del Subsistema de Seguridad y Privacidad de la Información la periodicidad para revisar las políticas del subsistema, lo que podría conllevar al incumplimiento del control A.5.1.2. de la ISO 27001:2013.

6.1.2. Organización de la Seguridad de la Información. (Dominio A.6 NTC-ISO/IEC 27001:2013)

6.1.2.1. A.6.1 Organización interna. Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

A.6.1.1 Roles y responsabilidades para la seguridad de información.

Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.

S.E. Se observó que la Unidad cuenta con el Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, código 02-02-DT-01, v.4, del 24-12-2018 del 24/12/2018, donde se encuentra el ítem *2.6. Roles y Responsabilidades del SGSI* donde, entre otros, se indican las funciones y responsabilidades asignadas al Comité Institucional de Gestión y Desempeño mediante la Resolución interna 890 del 13 de Julio del 2018, al Oficial de Seguridad de la Información (Profesional Especializado Grado 10 – Gerencia de Tecnología), las Gerencias, Subgerencias y Oficinas de la UAECD y, se enumeran las responsabilidades específicas asignadas a la Gerencia y Subgerencias de Tecnología, Subgerencia de Recursos Humanos, Subgerencia Administrativa y Financiera, Oficina Asesora Jurídica, Oficina de Control Interno, Terceras partes y, Funcionarios y contratistas de la UAECD.

S.E. Igualmente, en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. 29/10/2019, para cada una de las políticas allí consignadas, se indican las responsabilidades de las partes involucradas.

S.E. Con el fin de verificar el cumplimiento de las responsabilidades establecidas en el numeral *2.6.12 Funcionarios y contratistas de la UAECD* del Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, se aplicó una lista de verificación a 39 usuarios de un total de 245 (aprox. 16%), que desarrollan sus actividades en las áreas de Gerencia de Tecnología y sus 2 Subgerencias, Gerencia Comercial y de Atención al Usuario, Gerencia IDECA, Subgerencia Administrativa y Financiera, y la Subgerencia de Recursos Humanos, con los siguientes resultados por tema.

Tabla 1: Resultados consolidados aplicación listas de verificación usuarios.

Tema	Respuesta positiva o acertada	% con respecto al total
Gestión de Incidentes de Seguridad de la Información		
¿Sabe qué es un incidente de seguridad de la información?	28	72%
¿Sabe cuál es su responsabilidad frente a la gestión de incidentes?	26	67%
¿Conoce el procedimiento a seguir?	19	49%
Áreas Seguras		
¿Reconoce las áreas seguras de la Unidad?	28	72%
¿Conoce el procedimiento a seguir para acceder a estas áreas o en caso de que se presente algún incidente?	26	67%
Activos de Información		
¿Sabe qué es un activo de información y sus responsabilidades frente a los mismos?	20	51%
¿Cuáles activos de información produce, utiliza, procesa o tiene a su cargo? y qué nivel de confidencialidad tiene?	23	59%
¿Cómo los protege los activos de información?	21	54%
Mencione algunas reglas para el uso del correo electrónico.	21	54%
¿Conoce las Reglas para el uso de internet? Mencione	21	54%
Escritorio y Pantalla Limpios		
Conoce y aplica la política de escritorio y pantalla limpios	32	82%
Transferencia de Información		
¿Transfiere información interna o externamente?	29	74%
¿Conoce la política y los mecanismos para transferencia de información?	21	54%
Continuidad del Negocio		
¿Conoce la existencia del objetivo del Subsistema de Gestión de Continuidad del Negocio en la UAECD?	27	69%
Desde su puesto de trabajo, ¿conoce si pertenece a un equipo (roles y responsabilidades) de trabajo en el Subsistema de Gestión de Continuidad del Negocio?	12	31%

Elaboración propia del auditor.

No obstante, la información remitida a través del boletín interno de la Unidad y las capacitaciones realizadas por el grupo de Seguridad de la Información, los niveles de apropiación y cumplimiento de las responsabilidades del Subsistema de Seguridad y Privacidad de la Información por parte de los servidores públicos están por debajo del 60%.

Adicional a lo encontrado directamente con las preguntas de la lista de verificación, se encontraron las siguientes situaciones:

a) Llaves de los archivos de gestión sin salvaguarda.
b) Computadores desatendidos, sin usuario bloqueado.

c) Gran cantidad de documentos o expedientes sobre los escritorios, en especial en la Gerencia Comercial y de Atención al Usuario.
d) Desconocimiento de la ubicación de los documentos del Subsistema de Seguridad y Privacidad de la Información y de los procedimientos relacionados (gestión de incidentes, áreas seguras, entre otros).
e) Desconocimiento del archivo de activos de información y de las características de confidencialidad de la información que manejan o gestionan.
f) No tienen claridad en el concepto de "transferencia de información", durante la indagación sobre ese punto, los usuarios no tenían certeza de si transferían o no información, al explicarles el término, comentaban que sí hacían transferían información por múltiples canales de comunicación.

Recomendación:

Con el fin de aumentar los niveles de apropiación y conocimiento en el Subsistema de Seguridad y Privacidad de la Información, se deben revisar y replantear, junto con el apoyo de la Oficina Asesora de Comunicaciones, las estrategias de comunicación de las políticas, procedimientos y demás lineamientos relacionados con el Subsistema de Seguridad y Privacidad de la Información de la Unidad. Así mismo, los jefes de área deben propender por el fomento de la participación en las capacitaciones y la socialización de los lineamientos del SGSI.

Igualmente, se sugiere implementar una estrategia de cierre de brecha, aplicando una encuesta de conocimiento antes y después de cada capacitación, con el fin de determinar la efectividad de estas.

A.6.1.2 Separación de deberes.

Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

S.E. Adicional a lo mencionado en el punto anterior, en el Procedimiento Mantenimiento de aplicaciones, código 13-02-PR-19, del Proceso Provisión y Soporte de TI, se encuentran definidos y establecidos los roles y responsabilidades de los participantes (Líder Funcional, Líder Técnico, Analista de Desarrollo, Analista de Calidad, Usuario, entre otros) en los proyectos de desarrollo de software realizados al interior de la entidad. Estos procedimientos están soportados en el software Mesa de Servicios CA.

A.6.1.3 Contacto con las autoridades.

Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.

S.E. En entrevista con la Oficial de Seguridad se evidenció que el listado de contacto con las autoridades se encuentra en la base de datos de conocimiento de la mesa de servicios de TI.

A.6.1.4 Contacto con grupos de interés especial.

Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

S.E. En entrevista con la Oficial de Seguridad se evidenció que el listado de contacto con grupos de interés especial se encuentra en la base de datos de conocimiento de la mesa de servicios de TI.

A.6.1.5 Seguridad de la información en la gestión de proyectos.

Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.

S.E. La Unidad tiene establecido el Procedimiento Mantenimiento de aplicaciones, código 13-02-PR-19, v.5 del 02/05/2019, para la gestión de proyectos de software desarrollados por la entidad.

S.E. Igualmente, se cuenta con el Procedimiento Gestión de Riesgos Sobre los Activos en el Marco de la Seguridad de la Información, código 02-02-PR-03, V.4. del 04/07/2019, cuyo objetivo es "Realizar la identificación, valoración, análisis, evaluación y tratamiento de los riesgos de la seguridad de la información de la UAECD".

6.1.2.2. A.6.2 Dispositivos móviles y teletrabajo. Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.6.2.1. Política para dispositivos móviles.

Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

S.E. El control se encuentra documentado en el ítem 2.9. Política para Dispositivos Móviles del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02.

A.6.2.2 Teletrabajo.

Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

S.E. En la Declaración de Aplicabilidad, referencia el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, para el cumplimiento de este control, sin embargo, se evidenció que en la política *2.7. de Transferencia de la información*, se indica que: 2.7.4. Principios, (...) *f. Las actividades de teletrabajo en las cuales se requiera realizar transferencia de información deben cumplir igualmente con la política de transferencia de*

información y la Política de teletrabajo que establezca la Unidad. No obstante lo indicado, no se evidencia una política de teletrabajo.

S.E. Igualmente, se tiene documentado el Procedimiento Teletrabajo, asociado al proceso Gestión del Talento Humano. Código 06-05-PR-03, v. 3, del 10/05/2019.

Hallazgo:

(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció el incumplimiento de lo establecido en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, ítem 2.7.4. Principios, que indica que se debe cumplir con la política de teletrabajo que establezca la Unidad, sin embargo, la misma no ha sido determinada a la fecha de la auditoría.

6.1.3. Seguridad de los Recursos Humanos. (Dominio A.7 NTC-ISO/IEC 27001:2013).

6.1.3.1. A.7.1 Antes de asumir el empleo. Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1.1. Selección.

Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

S.E. Se observaron los siguientes documentos en el Sistema Integrado de Gestión, los cuales tienen actividades de verificación de antecedentes de las personas que se vincularán como funcionarios de la entidad:

- Procedimiento de Selección y Vinculación de Provisionales, código 06-01-PR-03, V.4, 21/10/2019, actividad *26. Verificar antecedentes del aspirante*.
- Procedimiento de Selección y Vinculación de Servidores de Libre Nombramiento y Remoción, código 06-01-PR-04, v.1, 08/11/2017, actividad *1.7 Verificar antecedentes del aspirante*.
- Procedimiento Selección y Vinculación Período de Prueba, código 06-01-PR-06, V.3, 29/10/2018, actividad *27. Verificar antecedentes del aspirante*.

S.E. Por otra parte, en el Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, numeral 2.4.3 Seguridad de los recursos humanos, ítem b. se establece que "*Antes de la contratación laboral o contractual, la Unidad deberá realizar el proceso de verificación de antecedentes de acuerdo con las leyes, reglamentos y ética pertinentes proporcional a la clasificación de la información a la que va a acceder el funcionario o contratista."*, lo que se implementó a través de la Circular interna 003 del 10/12/2018, punto 10. "*El abogado adelantará la consulta de los siguientes documentos y los respectivos certificados se anexarán a la plataforma en la plataforma tecnológica del Secop II:*

(...)", y se listan los certificados de antecedentes de la Policía Nacional, Personería, Procuraduría, Contraloría y Sistema Registro Nacional de Medidas Correctivas.

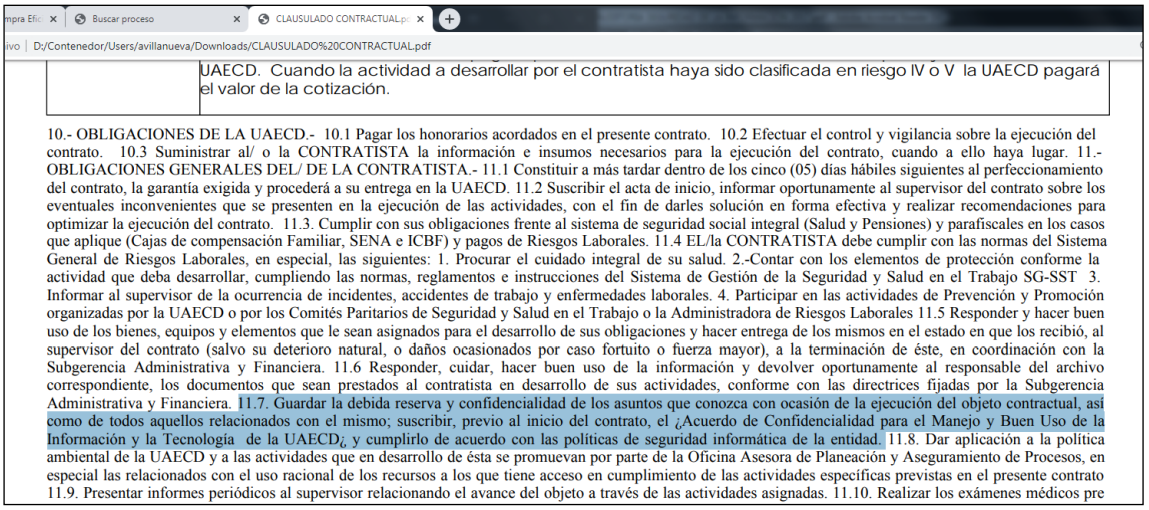
A.7.1.2 Términos y condiciones del empleo.

Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

S.E. Durante la revisión documental, se evidenció que el Acuerdo de Confidencialidad no se encuentra en el SIG, ni dentro de los documentos vigentes ni los obsoletos. Así mismo, se encontró que en el Procedimiento Contratación Directa, código 11-01-PR-05, actividades 21 y 22, mencionan "*Acuerdo de confidencialidad*".

S.E. Se verificó que, tanto los funcionarios (provisionales, carrera administrativa y, libre nombramiento y remoción) y los contratistas que ingresan a la entidad deben firmar el Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de la Unidad Administrativa Especial De Catastro Distrital - UAECD Servidores Públicos, código 06-01-FR-40, v.2, como requisito para la posesión del cargo o la aceptación del contrato, respectivamente, en la que se especifica que la persona "*debe conoce y dar cumplimiento a las políticas de seguridad de la información, continuidad del negocio y servicios tecnológicos que se encuentran consignadas en el Sistema de Gestión Integral – SGI de la UAECD y las normas e instrumentos establecidos para ello.".* Igualmente, los contratistas de prestación de servicios, persona natural y jurídica, tienen cláusulas de confidencialidad para este fin.

La OCI verificó 10 contratos de prestación de servicios persona natural vigencia 2019 en el SECOP, encontrando que tenían el respectivo Compromiso de Confidencialidad firmado, y la cláusula de confidencialidad de la información de la UAECD, como se observa en la siguiente imagen, tomada de uno de los contratos revisados (160-2019)



6.1.3.2. A.7.2 Durante la ejecución del empleo. Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

A.7.2.1 Responsabilidades de la dirección.

Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

S.E. A través del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, se asignan responsabilidades a los servidores públicos de la Unidad y se menciona en cada una de las políticas de seguridad de la información que: "*Todos los funcionarios o contratistas de Unidad, personal que labore en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad externa), que por su labor generen, custodien o tengan acceso a datos e información de la Unidad, así como a los diferentes recursos tecnológicos que los procesan, deben conocer y dar cumplimiento a la presente política*. (…)

El incumplimiento del FUNCIONARIO total o parcial de la presente política, podrá constituirse como falta disciplinaria y por lo tanto podrá dar lugar a la acción e imposición de la sanción correspondiente establecida en la ley PENAL, en el CODIGO DISCIPLINARIO ÚNICO y en las demás normas que se encuentren vigentes.

El incumplimiento de los CONTRATISTAS, PERSONAL QUE LABORE EN LAS INSTALACIONES VINCULADO CON PROVEEDORES DE LA UNIDAD O PERSONAL EXTERNO (EMPRESA O ENTIDAD EXTERNA), total o parcial de la presente política estará sujeto a las sanciones contractuales, civiles y/o penales a que haya lugar, por los daños y perjuicios causados a la Unidad o a terceros.".

S.E. Igualmente, como se mencionó en el control A.7.1.2 Términos y condiciones del empleo, los servidores públicos (funcionarios provisionales, de carrera administrativa, libre nombramiento y remoción y, contratistas) firman el Compromiso de Confidencialidad antes de iniciar sus actividades en el Unidad.

S.E. No obstante lo anterior, como se indicó en el control A.6.1.1 Roles y responsabilidades para la seguridad de información, los niveles de apropiación e implementación de los lineamientos del SGSI están por debajo del 60%.

Recomendación: Revisar las estrategias de implementación del control A.7.2.1 Responsabilidades de la dirección, con el fin de lograr una mayor efectividad en la exigencia de la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la entidad.

A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.

Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

S.E. En el Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, código 02-02-DT-01, v.4, 24/12/2018, numeral 2.4.3 Seguridad de los recursos humanos, ítem *g. La Unidad deberá asegurar que sus funcionarios y contratistas tomen conciencia de sus responsabilidades respecto a la seguridad de la información y las cumplan, para lo cual deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo*.

S.E. Se observó la realización de charlas sobre el Subsistema de Gestión de Seguridad y Privacidad de la Información y el Subsistema de Gestión de Continuidad del Negocio, de acuerdo con lo programado por la Oficial de Seguridad y su equipo de trabajo y, el Oficial de Continuidad del Negocio, para la vigencia 2019, a la fecha de la auditoría han asistido 236 personas, sin embargo, como se comenta en el control A.6.1.1 Roles y responsabilidades para la seguridad de información, los niveles de apropiación e implementación de los lineamientos del SGSI están por debajo del 60%, por lo tanto se ratifica la recomendación dada en el punto en mención.

A.7.2.3 Proceso disciplinario.

Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

S.E. Se encontró que la UAECD, tiene documentada la caracterización del Subproceso de Gestión Disciplinaria, código 15-SP-01, V.6 del 25/07/2019, dentro de la cual se establece que existen dos clases de procedimientos: Procedimiento Gestión Disciplinaria, código 15-01-PR-01, V.6 del 25/07/2019 y Procedimiento De Gestión Preventiva, código 15-01-PR-03, V.1 del 13/12/2018, y en el nomograma se encontró la referenciación de la Ley 1952 de 2019, "*Por medio del cual se expide el Código General Disciplinario se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el Derecho Disciplinario*."

S.E. Se observó, al momento de entrevista a la Profesional de la Subgerencia de Recursos Humanos, que tiene a cargo apoyar las investigaciones disciplinarias que lleva la Oficina de Control Disciplinario (apoyar en cuanto a aportar pruebas e información que tenga la Subgerencia de Recursos Humanos), que los documentos que se remiten a la Oficina en mención, no siguen los lineamientos para la Transferencia de Información establecidos en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, así mismo la carpeta compartida a través del fileserver, donde se guardan los documentos digitales, no tiene los requisitos de seguridad necesarios, y tienen acceso a ella las 24 personas que hacen parte de la Subgerencia de Recursos Humanos:

"*2.7.4. Principios (…)*
e. Para el caso de información clasificada o reservada, categorizada así de acuerdo con lo establecido en la Ley N° 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones", regulada mediante el Decreto N° 103 de 2015 "por el cual se reglamenta parcialmente la Ley N° 1712 de 2014 y se dictan otras disposiciones", se deben utilizar técnicas criptográficas que permitan proteger la confidencialidad, la integridad y la autenticidad de la información, de acuerdo con la política sobre el uso de controles criptográficos que se declare en la Unidad. (…)

2.7.4.1.1. Transferencia por correo electrónico

La información a transferir debe ser enviada a través de un archivo comprimido el cual debe estar cifrado, especialmente si la información es de carácter reservado o clasificado. (…)

2.7.4.1.4. Transmisión por correspondencia o en la mano

La transmisión de la información clasificada o reservada debe contar con una traza de dicho tránsito y ser entregada a la persona autorizada, haciendo uso de un mecanismo adecuado de entrega (correo certificado).

La información debe ser asegurada en un paquete etiquetado y debe contar con un sello el cual debe romperse al abrir el paquete.

El paquete debe tener una dirección de retorno y detalles del contacto, en caso de que no pueda ser entregado.

La etiqueta no debe indicar la naturaleza o el valor de su contenido.

Debe quedar constancia de la recepción del paquete por parte del destinatario (firma).
Se debe verificar el tiempo aproximado de entrega del paquete y luego de transcurrido el mismo verificar con el destinatario su recepción."

Hallazgo:

(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció el incumplimiento de los dispuesto en la Ley 734 de 2002, artículo 95, "*RESERVA DE LA ACTUACIÓN DISCIPLINARIA. En el procedimiento ordinario las actuaciones disciplinarias serán reservadas hasta cuando se formule el pliego de cargos o la providencia que ordene el archivo definitivo, sin perjuicio de los derechos de los sujetos procesales. (…)",* por cuanto los documentos, físicos y digitales remitidos desde y hacia la Oficina de Control Disciplinario, relacionados con investigaciones disciplinarias, no siguen los lineamientos establecidos para la transferencia de información clasificada y/o

reservada, lo que conlleva a que personas ajenas a la investigación tengan acceso a la documentación e información.

6.1.3.3. A.7.3. Terminación o cambio de empleo. Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.

A.7.3.1. Terminación o cambio de responsabilidades de empleo.

Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.

S.E. En el Procedimiento Gestión de Accesos, código 13-02-PR-04, V.6 del 10/06/2019, 3. Condiciones especiales de operación, numeral 3.1.1. Novedades de personal y contractuales, se indican los lineamientos que se deben aplicar en el caso de la terminación de un contrato, un retiro definitivo de un funcionario, el cambio de área de un usuario, entre otras.

S.E. En el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. 29/10/2019, numeral 2.2. Política Control de Acceso, 2.2.5. Responsabilidades, indica que una de las responsabilidades de los usuarios es "*2) Suscribir el documento "Compromiso de confidencialidad para el manejo y buen uso de la información y la tecnología de la Unidad Administrativa Especial de Catastro Distrital – UAECD" con la Unidad, el cual está publicado en el Sistema de Gestión Integral - SGI y es suministrado durante la vinculación a la Unidad (aplica para funcionarios, contratistas y usuarios de entidades externas que requieran acceder a un sistema de información de la Unidad).*".

6.1.4. Gestión de Activos. (Dominio A.8 NTC-ISO/IEC 27001:2013)

6.1.4.1. A.8.1 Responsabilidad por los activos. Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.

A.8.1.1 Inventario de activos.

Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

S.E. Se observó que la Unidad tiene documentados procedimientos para la administración de los Activos de información entre ellos se encuentra el de Actualización de Tablas de Retención Documental código 08-02-PR-01, Gestión de Activos en el Marco de la Seguridad de la Información código 02-02-PR-02, 02-02-PR-03 Procedimiento Gestión de Riesgos sobre los Activos en el Marco de la Seguridad de la Información, Inventario General de Activos código 02-02-FR-07 y una Matriz de Riesgos de Seguridad de la Información código 02-02-FR-08. Así mismo, en el Documento Técnico Manual del Subsistema de Gestión de Seguridad y

Privacidad de la Información, código 02-02-DT-01, se dan lineamientos al respecto en el numeral 2.4.4 Gestión de activos.

S.E. Gestión de Activos en el Marco de la Seguridad de la Información, establece la metodología para efectuar el inventario y la clasificación de los activos de información, para los diferentes tipos de activos de información que conforman la cadena de valor de la Unidad e indica los tipos en los que se dividirán los activos de información: datos o información, hardware, software, servicios, recurso humano o conocimiento, entre otros.

S.E. Así mismo se pudo evidenciar que el registro de activos de información- RAI- se encuentra publicado en el módulo de Transparencia y Acceso a la Información de la página web de la Unidad, enlace https://www.catastrobogota.gov.co/instrumentos-de-gestion?field_clasificacion_target_id=175. En entrevista con la Oficial de Seguridad indicó que, en desarrollo del plan de trabajo 2019, se está liderando el proceso de actualización los activos de información y a la fecha de la auditoría, de 17 dependencias se encuentra pendiente por entregar el archivo final la Subgerencia de Recursos Humanos.

A.8.1.2 Propiedad de los activos

Control: Los activos mantenidos en el inventario deben tener un propietario.

S.E. Se observó en los archivos de registro de activos de información publicados en la página web de la UAECD, una casilla denominada "*Propietario de los Activos*" y una columna "*Custodio de la Información*".

A.8.1.3 Uso aceptable de los activos.

Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

S.E. Se observó que en el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, código 02-02-DT-02, se encuentra incluido el numeral 2.6. Política de Uso Aceptable, a través de la cual se busca que se apliquen las reglas básicas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información por parte del personal (servidores públicos, personal tercerizado, etc.) que desarrolla actividades en la Unidad.

A.8.1.4 Devolución de activos.

Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

S.E. A través del Documento Técnico Manual del Subsistema de Gestión de Seguridad y Privacidad de la Información, código 02-02-DT-01, numeral 2.4.4 Gestión de activos, se indica que *(…) d. Todos los funcionarios, contratistas y personal que labora en las instalaciones vinculado con*

un proveedor de la UAECD deberán devolver todos los activos de la Unidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. e. El proceso de terminación deberá formalizar la devolución de todos los activos físicos y electrónicos entregados previamente, que son propiedad de la Unidad o que se le han confiado a ella.

S.E. Para lo anterior se observó que la Entidad tiene documentado diferentes lineamientos para la devolución de activos de información así: Procedimiento Traslado y Entrega de Elementos Devolutivos (asociado al proceso Provisión y Soporte De Servicios TI), código 07-01-PR-02, V.2, 19/09/2017, Instructivo Alistamiento y Entrega de Equipos de Escritorio, código 13-02-IN-06, V.3., 08/08/2018, y el formato Constancia para Entrega de Bienes y/o Elementos Asignados y Documentos, código 07-01-FR-04, v.2, 19/09/2017.

S.E. Por otra parte, no obstante los documentos antes mencionados, no se evidencia la estrategia de verificación de devolución de los activos físicos, ni para contratistas ni para funcionarios, teniendo en cuenta que en el formato "Constancia para Entrega de Bienes y/o Elementos Asignados y Documentos", no se indica la devolución de expedientes o carpetas de archivo asignadas o en préstamo.

Así mismo, se evidencia ambigüedad en el uso del término "*servidor público*", puesto que en el formato se excluye a los contratistas como servidores públicos: en el punto *Evaluación del Desempeño Laboral a la fecha del retiro (Servidores públicos)*, y en el procedimiento Traslado y Entrega de Elementos Devolutivos se indica: *servidor público en la modalidad de prestación de servicios (contrato).*

S.E. Finalmente, no hay claridad en cuanto a qué área debe archivar el formato una vez diligenciado por los contratistas o si el mismo debe ser o no tramitado, ya que en el Procedimiento Traslado y entrega de elementos devolutivos, 07-01-PR-02, Condiciones Especiales de Operación, se indica que "*Cuando finalice la vinculación de un servidor público en la Entidad, el funcionario deberá diligenciar y hacer firmar el formato "Constancia para entrega de bienes y/o elementos asignados y documentos" (...) Este formato debe ser entregado por el servidor (...) a su jefe inmediato, quien se encargará posteriormente de entregarlo a la Subgerencia de Recursos Humanos*", así las cosas se estarían excluyendo a los contratistas del diligenciamiento del formato una vez se finalice la ejecución contractual. Por otra parte, en la nota al final de la Constancia para entrega de bienes, se indica *"(...) debe remitir este formato junto con los demás documentos a la Subgerencia de Recursos Humanos, en caso de que sea un servidor público, o a la Oficina Asesora Jurídica en caso de que sea un contratista para que repose en la respectiva historia laboral o en la carpeta del contrato que corresponda*.".

Recomendación: Revisar el Procedimiento Traslado y entrega de elementos devolutivos y el formato Constancia para Entrega de Bienes y/o Elementos Asignados y Documentos, código 07-01-FR-04, con el fin de unificar términos y aclarar lineamientos, para evitar confusiones al momento de su diligenciamiento y custodia.

Hallazgo:

(OM) A partir de la auditoría al SGSI de la UAECD 2019, se observó que los archivos documentales no están incluidos en el formato "Constancia para Entrega de Bienes y/o Elementos

Asignados y Documentos", código 07-01-FR-04, v.2, 19/09/2017, lo que podría conllevar a la pérdida de expedientes documentales de la Unidad al momento del retiro de servidores públicos (contratistas, provisionales, carrera administrativa o libre nombramiento y remoción).

6.1.4.2. A.8.2 Clasificación de la información. Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

A.8.2.1. Clasificación de la información

Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

S.E. La entidad tiene documentado el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, V.5. del 24/12/2018, y en su numeral 3.3. Clasificación de Activos, se indica la clasificación de la información que produce la Unidad con respecto a la confidencialidad, a la integridad y a su disponibilidad.

A.8.2.2 Etiquetado de la información.

Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

S.E. La entidad tiene documentado el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, V.5. del 24/12/2018, y en su numeral 3.4.5. Etiquetado de activos, muestra una tabla con la clasificación y el etiquetado, tanto para medios electrónicos como físico, de la información de la Unidad.

S.E. Se evidenció el etiquetado de la información física a través de los formatos Rótulo para Carpeta código 08-03-FR-03 y Rótulo Para Cajas código 08-03-FR-02. Así mismo, el gestor de contenidos (WCC), tiene un metadato para el etiquetado de la información que se encuentra en proceso de parametrización y se creó la tabla de control de accesos (perfiles/roles) para el gestor de contenidos, que se encuentra en la Gerencia de Tecnología para su implementación. Por otra parte, se observó que la documentación contenida en las carpetas del fileserver, no tienen el etiquetado requerido, la información es compartida por todo el personal del área a la cual pertenece la carpeta.

Hallazgo:
(AC) A partir de la auditoría al SGSI de la UAECD 2019, se observó que la documentación contenida en las carpetas del fileserver, no tienen el etiquetado requerido, la información es compartida por todo el personal del área a la cual pertenece la carpeta, incumpliendo lo establecido en el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, numeral 3.4.5. Etiquetado de activos, lo que puede conllevar a que no se sigan los lineamientos normativos para el manejo de la información de acuerdo con su confidencialidad.

A.8.2.3 Manejo de activos.

Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

S.E. La entidad tiene documentado el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, V.5. del 24/12/2018, y en su numeral 3.4. Manejo de activos, da los lineamientos sobre las restricciones de acceso que el propietario del activo debe definir y revisar periódicamente, al igual que debe establecer los receptores autorizados de los activos, así mismo se define la protección de copia de información y el almacenamiento de activos tipo hardware.

S.E. Se observó que, mediante el aplicativo CORDIS, se realiza la radicación y control de los documentos que se reciben en la UAECD y de los documentos generados por la entidad, al igual que de los trámites internos para dar respuesta a los diferentes requerimientos. Así mismo, se aprobó la implementación del gestor documental de contenidos (WCC) para una nueva versión del CORDIS. Para la vigencia del 2019 se ha venido implementado el desarrollo "módulo/ funcionalidad CORDIS" como gestor de contenidos, el cual se encuentra ubicado en la intranet de la Unidad, módulo de servicios, link: http://infodoc.catastrobogota.gov.co/infodocweb/Login.aspx, integrando así el Proceso de Gestión Documental, el Subproceso Gestión de Correspondencia y los demás aplicativos de la UAECD en el gestor de contenidos (WCC).

S.E. Por último, la Unidad está desarrollando un Sistema Integrado de conservación que permita la preservación de la información, como uno de los aspectos clasificados como más críticos en el Plan Institucional de Archivo – PINAR, para lo cual realizó la contratación de una profesional, que tiene por objeto: "*Prestar los servicios profesionales para la elaboración del sistema Integrado de Conservación Documental y proponer un cronograma general de actividades con un plan de trabajo, revisión de documentos con un diagnóstico, elaborar un programa de inspección y mantenimiento de instalaciones*." y el cual finaliza en el de diciembre de 2019.

6.1.4.2. A.8.3 Manejo de medios. Objetivo: Los medios deben ser controlados y protegidos. Establecer los procedimientos operativos adecuados para proteger los documentos, los medios informáticos, datos de entrada o salida y documentos del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizados.

A.8.3.1 Gestión de medio removibles.

Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

S.E. Se observó que la entidad tiene documentado el Procedimiento Gestión de Medios Removibles, código 13-02-PR-30, V.1. del 09/06/2017, asociado al Proceso de Provisión y Soporte de Servicios de TI, a través del cual se dan lineamientos para la protección de los medios removibles (CDs, DVDs, memorias de almacenamiento, cintas magnéticas, discos removibles, rollos de microfilmación, medios impresos, entre otros), donde la Unidad guarda

información, con el fin de evitar la divulgación o modificación de la información que ellos contienen y el retiro o destrucción no autorizados de los mismos.

S.E. Se evidenció el Procedimiento Baja de Elementos Devolutivos, código 07-01-PR-04, para el caso de los medios removibles de la Unidad, que son considerados obsoletos o con daño irreparable, y que deben ser dados de baja de acuerdo con lo establecido en dicho procedimiento.

A.8.3.3 Transferencia de medios físicos.

Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

S.E. Se observó que la entidad tiene establecida la Política de Transferencia de información en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, en cuyo ítem 2.7.4.1.3. da los lineamientos para la "*Transferencia a través de medios removibles (CD1, DVD2, USB3, Tarjeta de memoria)*."

S.E. Se evidenció el Procedimiento Gestión de Medios Removibles, código 13-02-PR-30, V.1, 09/06/2017, proceso Provisión y Servicios de TI, en cuyo ítem 3.1.5. Condiciones para el almacenamiento, transporte y control de medios removibles, 3.1.5.3. Condiciones requeridas durante el transporte, se dan los lineamientos propios para el traslado físico de los medios removibles de propiedad de la UAECD, desde y hacia el sitio de almacenamiento provisto para ellos.

S.E. Finalmente, para el caso de transferencia de archivos físicos, se tiene el Instructivo Administrar y Transferir Archivos de Gestión, código 08-03-IN-02, asociado al proceso de Gestión Documental.

6.1.4. Control de Accesos. (Dominio A.9 NTC-ISO/IEC 27001:2013)

6.1.4.1. A.9.1 Requisitos del negocio para el control de acceso. Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

A.9.1.1 Política de control de acceso.

Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.

S.E. La OCI observó que, en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, V.6. del 29/10/2019, se encuentran establecidos los lineamientos con respecto al control de acceso de los activos de información, numeral 2.2 Política de control de acceso.

[2] Disco Versátil Digita - DVD (Por sus siglas en inglés Digital Versatile Disc)
[3] Bus Universal en Serie - USB (Por sus siglas en inglés Universal Serial Bus

A.9.1.2 Política sobre el uso de los servicios de red.

Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

S.E. La entidad tiene documentadas las 2.2. Control de Acceso y 2.6 Uso aceptable, en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. del 29/10/2019, las cuales incluyen, principios y responsabilidades para el manejo de accesos a la información de la Unidad, incluyendo los servicios de red, así como el buen uso de los recursos tecnológicos donde los activos de información deben ser utilizados únicamente en el ejercicio de las funciones asignadas o de las obligaciones contractuales establecidas con la Unidad.

S.E. Igualmente, la entidad tiene documentado en el Procedimiento Gestión de Accesos, código 13-02-PR-04, V.6, 10/06/2019, asociado al proceso de Provisión y Servicios de TI, el numeral 3.11. Control de acceso a los recursos de red.

S.E. Adicionalmente, la Unidad tiene implementados controles a través de la autenticación de los usuarios a la red a través del Directorio Activo – DA, bloqueo de sitios web a través del firewall, parámetros en el firewall para no permitir la intrusión de usuarios externos no autorizados, entre otros.

6.1.4.2. A.9.2. Gestión de acceso de usuarios. Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

A.9.2.1. Registro y cancelación del registro de usuarios.

Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

S.E. En el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, se detallan los principios y las responsabilidades en cuanto al cumplimiento de la Política Control de Acceso, entre las que se mencionan las solicitudes de acceso a la información de la Unidad, restricciones y controles a los permisos asignados a las cuentas de usuario, lineamientos para el traslado o retiro de un funcionario o la terminación de un contrato, entre otros.

S.E. Se observó que, en las Condiciones especiales de operación del Procedimiento Gestión de Accesos, código 13-02-PR-04, numeral 3.1.1. Novedades de personal y contractuales, se dan los lineamientos necesarios para la creación y cancelación de usuarios de red o de aplicativos utilizados en la Unidad.

A.9.2.2 Suministro de acceso de usuarios.

Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.

S.E. A través del Procedimiento Gestión de Accesos, código 13-02-PR-04, se gestiona la creación, activación, desactivación y/o modificación de las cuentas de usuario, sus privilegios o permisos para el acceso a la información y a los diferentes recursos tecnológicos que soportal los servicios de TI de la UAECD y el formato Solicitud Cuentas de Usuario, código 13-02-FR-04, es utilizado para para dicha gestión y debe ser diligenciado por el jefe de la dependencia correspondiente, a través de la mesa de servicios de TI.

A.9.2.3 Gestión de información de autenticación secreta de usuarios.

Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

S.E. Se encontró que se asignan cuentas de usuario privilegiadas a los administradores de recursos tecnológicos, a las cuales, de acuerdo con lo establecido en el Procedimiento Gestión de Accesos, código 13-02-PR-04, numeral 3.6. Depuraciones y revisiones periódicas, "*d) Revisiones de las cuentas de usuario privilegiadas asignadas a los administradores de recursos tecnológicos y sus permisos se realizarán semestralmente. (…) gestor de accesos valida cuentas privilegiadas para continuar o ser depuradas."* Así mismo, en el numeral 3.9. Administración de cuentas de usuario, se indica que *(...) Los privilegios de administración sobre los equipos de cómputo deberán ser asignados únicamente a personal de la mesa de servicios de TI, cualquier excepción deberá ser aprobada por el Gestor de Accesos. La cuenta de administración sobre los equipos de cómputo deberá ser custodiada por la Subgerencia de Infraestructura Tecnológica y deberá cambiarse su contraseña cada 3 meses. (...)*

A.9.2.4 Gestión de información de autenticación secreta de usuarios.

Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.

- En el numeral 3.5. Notificaciones del Procedimiento Gestión de Accesos, código 13-02-PR-04, se indica que al resolver la solicitud en la mesa de servicios de TI, se notifica al jefe de dependencia la gestión realizada (creación, modificación, eliminación de usuarios) a través de correo electrónico, mediante una notificación manual interna generada desde la mesa de servicios de TI, al funcionario, contratista, personal que labora en las instalaciones vinculado con un proveedor de la entidad que tiene asignadas dichas cuentas de usuario y las acciones realizadas sobre sus permisos o contraseñas. Así mismo, se evidenció que la clave inicial de un usuario es entregada en sobre sellado con los datos de usuario y clave asignados.

A.9.2.5 Revisión de los derechos de acceso de usuarios.

Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

S.E. Se evidenciaron los correos remitidos por la Subgerente de Infraestructura Tecnológica a los jefes de dependencia, con el fin de que se realicen las revisiones periódicas de las cuentas de

usuario y sus permisos, como se indica en el numeral 3.6. Depuraciones y revisiones periódicas del Procedimiento Gestión de Accesos, código 13-02-PR-04. Sin embargo, en el procedimiento se indica que quien debe remitir los correos es el gestor de accesos, no el Subgerente de Infraestructura Tecnológica.

Recomendación: Revisar el ítem 3.6. Depuraciones y revisiones periódicas del Procedimiento Gestión de Accesos, y determinar si la responsabilidad de la depuración cuatrimestral y la semestral (en el caso de las cuentas privilegiadas) las debe realizar el gestor de accesos.

A.9.2.6 Retiro o ajuste de los derechos de acceso.

Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

S.E. Se observó que el retiro o ajuste de los derechos de acceso se encuentra documentado en los numerales 3.1.1. Novedades de persona y contractuales y, 3.9. Administración de cuentas de usuario del Procedimiento Gestión de Accesos, código 13-02-PR-04. Se observó a través de correos electrónicos, que posterior a la depuración de usuarios realizada por los jefes de dependencia, y la realizada por los administradores de recursos tecnológicos, se efectúa la eliminación de usuarios que ya no se encuentran desarrollando actividades en la entidad.

6.1.4.3. A.9.3 Responsabilidades de los usuarios. Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

A.9.3.1 Uso de información de autenticación secreta.

Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

S.E. En el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, se observan las responsabilidades sobre el uso de claves y la información a la cual se tiene acceso en la Unidad, con el fin de dar cumplimiento a la Política Control de Acceso, numeral 2.2.

S.E. Por otra parte, se evidenció que los equipos portátiles, tanto los que se encuentran asignados a la Gerencia de Tecnología, como los que reposan en las salas de juntas, tienen adherido un papel con el usuario y clave correspondiente, que dan acceso a la carpeta de red temporal, donde se puede encontrar diversa información de las áreas de la Unidad, sin ninguna restricción, como se muestra en las siguientes imágenes:

Imagen 1. Imagen de portátil Lenovo 5

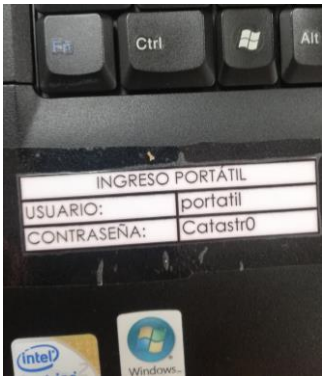
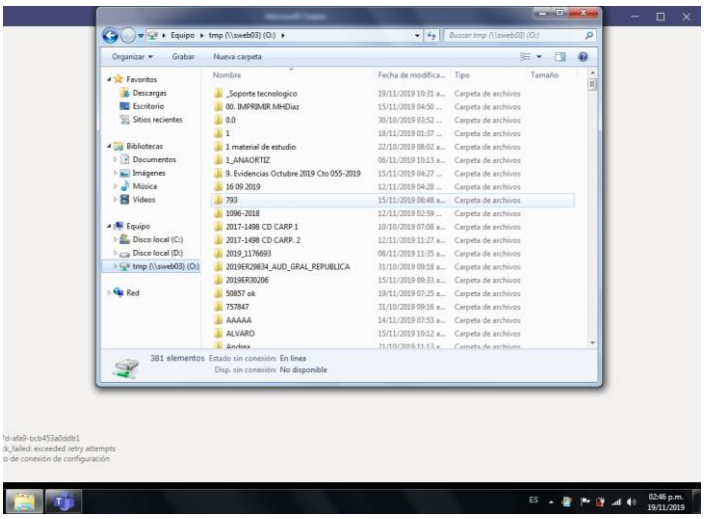


Imagen 2. Prueba de equipo portátil conectado a la red de la entidad.



Hallazgo:

(OM) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció que, a través de los usuarios y claves adheridas en los portátiles asignados a la Gerencia de Tecnología, como los que reposan en las salas de juntas, se puede tener acceso a la información que reposa en la carpeta de red denominada "temporal", lo que podría generar un incumplimiento a lo establecido en el numeral 2.2. Política de Control de Acceso del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información en cuanto a la utilización de información de la Unidad por personas no autorizadas.

6.1.4.4. A.9.4 Control de acceso a sistemas y aplicaciones. Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1 Restricción de acceso a la información. **Control**: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso y A.9.4.2 Procedimiento de ingreso seguro. **Control**: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.

S.E. A través del Procedimiento Gestión de Accesos, código 13-02-PR-04, se dan los lineamientos para la asignación de privilegios o permisos a los usuarios para el acceso a la información y a los diferentes recursos tecnológicos que soportan los servicios de TI. Adicionalmente se tiene restringido el uso de dispositivos de medios de almacenamiento (USB), el cual solo puede ser autorizado por el jefe de la dependencia. Lo anterior, se evidenció durante el seguimiento realizado por la Oficina de Control Interno para el informe de Derechos de Autor Software durante el mes de octubre, donde se verificaron las restricciones de acceso de 64 usuarios.

A.9.4.3 Sistema de gestión de contraseñas.

Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

S.E. La entidad tiene documentado la estándar generación de contraseñas, la administración de cuentas de usuario y la administración de contraseñas en el Procedimiento Gestión de Accesos y se encuentra implementado a través del servidor de dominio, que solicita modificación de contraseña cada 3 meses, número de intentos permitidos antes de bloquearse, repetición de contraseñas, entre otros parámetros.

A.9.4.4 Uso de programas utilitarios privilegiado.

Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

S.E. Se evidenció el listado de software libre autorizado por la Unidad en el CMDB administrado por la Gerencia de Tecnología, el cual es actualizado por la Oficial de Seguridad. Así mismo, tal y como manifestó la Gerencia de Tecnología en el mes de octubre de 2019, para el informe de Derechos de Autor Software, la Unidad tiene implementados los siguientes controles: "*i. Por política del Directorio Activo se restringe la instalación de software para todos los usuarios finales y solo se puede hacer con usuarios que cuenten con permisos de administrador de red y administrador local, ii. Se tienen el reporte del Software con que cuenta cada uno de los equipos de cómputo que están matriculados a la red, y que mediante el Agente de CA es reportado y sobre el cual se realiza una revisión y depuración. iii. A nivel de la plataforma de Antivirus se tienen configuradas reglas de bloqueo de instalación de Software que se considera malicioso y no autorizado, el cual se alimenta de acuerdo con el software que se reporta como no autorizado. iv. En el "Instructivo Instalación o Desinstalación de Software" 13-02-IN-09-v.2, publicado en el SGI, se indican los principios a tener en cuenta en lo relacionado con la instalación y desinstalación de software.*".

A.9.4.5 Control de acceso a códigos fuente de programas.

Control: Se debe restringir el acceso a los códigos fuente de los programas.

S.E. La Unidad cuenta con la Política de desarrollo seguro, establecida en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02 y con el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01,V.1 del 20/09/2018, a través de los cuales se establecen los controles de seguridad y privacidad de la información para el desarrollo de sistemas de información nuevos o mejoras a los ya existentes.

6.1.5. Criptografía. (Dominio A.10 NTC-ISO/IEC 27001:2013)

6.1.5.1. A.10.1 Controles criptográficos. Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

A.10.1.1. Política sobre el uso de controles criptográficos. **Control**: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información y A.10.1.2. Gestión de llaves. **Control**: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

S.E. La entidad tiene establecida la Política para el uso de controles criptográficos en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, que incluye las responsabilidades asignadas para el cumplimiento de la política y la gestión de llaves. Esta política fue socializada en el mes de octubre de 2019 y se encuentra en proceso de implementación.

6.1.6. Seguridad física y del entorno. (Dominio A.11 NTC-ISO/IEC 27001:2013)

6.1.6.1. A.11.1 Áreas seguras. Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

A.11.1.1. Perímetro de seguridad física.

Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.

S.E. La entidad cuenta con la Política de Control de Acceso, plasmada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, que tiene como uno de sus objetivos específicos "*Establecer las actividades y condiciones para el acceso a las instalaciones y áreas seguras de la Unidad Administrativa Especial de Catastro Distrital – UAECD, con el fin de ejercer el control físico durante el ingreso, permanencia y retiro de funcionarios, contratistas, personal que labora en las instalaciones de la Unidad vinculado con un proveedor de la unidad y visitantes a dichas áreas*.".

S.E. Así mismo, se tiene documentado el Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06, V.1 del 03/09/2019.

S.E. Actualmente, se encuentra en ejecución el contrato 304-2019 con SOFTWARE AUTOMATION AND TECHNOLOGY LTDA-SAUTECH LTDA, cuyo objeto es "*Adquirir el sistema de control de accesos para las áreas de la UAECD."*, por valor de $137.150.000 y que entre otras obligaciones específicas tiene "*Entregar a la UAECD debidamente instalado, configurado y en perfecto estado de funcionamiento todos los elementos adquiridos en el contrato*" (lectores biométricos, electroimanes, botones de salida y software de control de

accesos, tiempos y asistencias), con una duración de 45 días hábiles y que dio inicio el 09 de septiembre de 2019.

A.11.1.2. Controles físicos de entrada.

Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

S.E. Adicional a lo descrito en el punto anterior, se observó el Instructivo Operación del Sistema de Control de Acceso, código 07-03-IN-04, V.4. del 26/09/2019, sin embargo, se evidenció que, de acuerdo con lo informado por el Subgerente Administrativo y Financiero a través de correo electrónico del 30/10/2019, el control de acceso existente hasta el mes de septiembre de 2019 no guardaba registro desde el año 2017 por obsolescencia, por lo tanto, no se estaba dando cumplimiento a las actividades del ítem "*D. Reporte mensual de control de acceso.*"

Hallazgo
(OM) A partir de la auditoría al SGSI de la UAECD 2019, revisar y actualizar el Instructivo Operación del Sistema de Control de Acceso, código 07-03-IN-04, por cuanto en la actividad 7. Entregar carné y mecanismo de acceso, sólo se menciona como responsable de la actividad a "*funcionario en proceso de desvinculación*", excluyendo a los contratistas. Así mismo, de ser necesario, el instructivo debe ser adaptado al nuevo sistema de control de acceso. Por último, se deben crear lineamientos para el manejo del sistema de acceso: especificar qué área y qué personal quedará a cargo de su administración, condiciones de seguridad para su manejo, reportes, entre otros.

A.11.1.3 Seguridad de oficinas, recintos e instalaciones.

Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

S.E. Aplica la situación evidenciada en el control A.11.1.1. Perímetro de seguridad física.

A.11.1.4 Protección contra amenazas externas y ambientales

Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

S.E. Se observó el documento "*INFORME IDENTIFICACIÓN CONTROLES REQUERIDOS PARA LA PROTECCIÓN DE LA UNIDAD CONTRA AMENAZAS EXTERNAS Y AMBIENTALES*" del 05/12/2017, sin embargo, no se evidenció el responsable o área quién lo generó. Adicionalmente, no se encontró el seguimiento a las brechas identificadas en la Tabla 3. del documento "*Identificación del estado actual de implementación de los controles contra amenazas externas y ambientales*".

S.E. La entidad cuenta con el contrato 224-2019 con AXA COLPATRIA, a través del cual se adquirió la póliza de seguro multirriesgo No. 1350, vigente del 19/04/2019 al 23/04/2020, que

cubre todo riesgo daño material, incluidos los equipos de cómputo y demás componentes de la arquitectura tecnológica de la UAECD.

Recomendación: Efectuar seguimiento a las brechas identificadas en la Tabla 3. del documento "*Identificación del estado actual de implementación de los controles contra amenazas externas y ambientales*", con el fin de establecer el estado actual de la implementación de dichos controles.

A.11.1.5. Trabajo en áreas seguras.

Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.

S.E. Además del Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06, se cuenta con el Formato Control de Personas que Ingresan a las Instalaciones de la Unidad con Autorización, código 07-03-FR-11, V.2 del 21/08/2019.

S.E. Se evidenció que el procedimiento es específico en cuanto a las indicaciones para el ingreso y salida de personal de las áreas seguras de la entidad, sin embargo, no se observan instrucciones de seguridad para llevar a cabo trabajos, operaciones o tareas en estas áreas y que puedan conllevar riesgo si no se realizan de manera adecuada.

Hallazgo:
(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció que el Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06, no incluye instrucciones de seguridad para llevar a cabo trabajos, operaciones o tareas en estas áreas, como lo indica el control de la ISO 27001:2013, A.11.1.5, lo que podría generar posibles riesgos a la seguridad de la información.

A.11.1.6. Áreas de despacho y carga.

Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

S.E. La entidad incluyó en las Condiciones especiales de operación del Procedimiento Administración de Bienes Muebles, código 07-01-PR-01, V.4 del 08/08/2019, la indicación de que "*Todo elemento que ingresa o sale de las áreas de despacho y carga debe ser relacionado en el formato 42-F.03 – Autorización de movimientos de bienes devolutivos, consumo y otros, el cual debe ser firmado por un servidor público y/o contratista de la Unidad quien se encuentre registrado en el formato 42-F.08 – Actualización de firmas autorizadas para solicitar servicios.*", así mismo menciona que "*El responsable de las áreas físicas de despacho y carga es la Secretaria Distrital de Hacienda, es quien establece las directrices y controles necesarios para el acceso de forma segura.*".

6.1.6.2. A.11.2. Equipos. Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

A.11.2.1. Ubicación y protección de los equipos

Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.

S.E. En entrevista con la Oficinal de Seguridad, indicó que la Subgerencia de Infraestructura cuenta con la topología de red de infraestructura crítica de la UAECD y la herramienta de IT CLIENT contiene la configuración de los equipos y alerta ante las modificaciones que se presenten.

A.11.2.2. Servicios de suministro.

Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

- En entrevista con la Oficinal de Seguridad, manifestó que la Unidad cuenta con servicio de UPS en los pisos 11, 12 y piso 2 y, la UPS del Datacenter que se encuentra en la Secretaria Distrital de Hacienda – SDH. Esta información se encuentra registrada en la documentación que conforma el Subsistema de Gestión de Continuidad del Negocio.

A.11.2.3. Seguridad del cableado.

Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.

S.E. Se observó el "*INFORME CON EL RESULTADO DE LA REVISIÓN FÍSICA REALIZADA AL CENTRO DE CABLEADO Y EQUIPOS DE COMUNICACIONES*" del 12/12/2017, en el que se tomó una muestra de 3 centros de cableado: 1) Centro de cableado Supercade Bosa. 2) Centro de cableado Torre B, piso 2 y 3) Datacenter (Centro de cómputo) Torre B, piso 2.
S.E. No se encontró un documento con la revisión de los 7 centros de cableado restantes.

Recomendación: Considerar la pertinencia de la revisión de los 7 centros de cableado que no fueron incluidos en el "*INFORME CON EL RESULTADO DE LA REVISIÓN FÍSICA REALIZADA AL CENTRO DE CABLEADO Y EQUIPOS DE COMUNICACIONES*" del 12/12/2017.

A.11.2.4. Mantenimiento de equipos.

Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

S.E. La entidad, a través del contrato 213-2018 con ORIGEN SOLUCIONES INFORMÁTICAS Y DE SOFTWARE SAS, cuyo objeto es: "*Servicio integral de mantenimiento con bolsa de*

repuestos, y soporte técnico para equipos de cómputo de escritorio y periféricos.", vigente hasta el 30/03/2020, realiza el mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad, adicional a los contratos específicos para el mantenimiento de los servidores y demás elementos activos de la infraestructura tecnológica.

A.11.2.5. Retiro de activos. **Control**: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa. A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones.

Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

S.E. En entrevista con la Oficinal de Seguridad, se observó la elaboración propuesta del Instructivo para la protección de equipos fuera de la entidad, la cual ha sido revisada con la Subgerencia Administrativa y Financiera.

S.E. La Unidad tiene documentado el Instructivo Cifrado de Información de Archivos, código 13-02-IN-10, V.1 del 22/12/2017, asociado al proceso de Provisión y Soporte de Servicios TI, sin embargo, el instructivo no menciona que el cifrado se debe aplicar como medida de seguridad a los activos que se encuentran o se lleven fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

Recomendación: Evaluar la propuesta del Instructivo para la protección de equipos fuera de la entidad y, de ser positiva, gestionar su formalización y socialización. Así mismo, relacionarlo con el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, código 02-02-PR-02, con el fin de proteger los activos de información que salen de las instalaciones de la entidad. Actualizar la información en la Declaración de Aplicabilidad.

A.11.2.7. Disposición segura o reutilización de equipos.

Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.

S.E. La UAECD tiene documentado el Procedimiento Baja de Elementos Devolutivos, código 07-01-PR-04, V.5 del 28/06/2019, y menciona en las Condiciones Especiales de Operación, *h) En el caso de los recursos tecnológicos (…) Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización*."

S.E. Por otra parte, se observó que, en el Procedimiento Traslado y Entrega de Elementos Devolutivos, código 07-01-PR-02, V.2 del 19/09/2017, asociado al Proceso Gestión de Servicios Administrativos, no se dan lineamientos en cuanto a la verificación de los medios de

almacenamiento de los equipos de cómputo que siguen en uso y que se trasladan de una persona a otra.

Recomendación: Revisar el Procedimiento Traslado y Entrega de Elementos Devolutivos, código 07-01-PR-02, e incluir los lineamientos para la verificación de los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.

A.11.2.8. Equipos de usuario desatendidos.

Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.

S.E. Se observó que, dentro de los principios de la Política de Escritorio y Pantalla Limpios, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. del 29/10/2019, se indica que "*b) Se deben bloquear los dispositivos móviles cuando se encuentren desatendidos, e) Toda sesión de trabajo en los equipos de cómputo o terminales en la Unidad se debe bloquear o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña cuando no estén siendo atendidos y debe activarse automáticamente luego de tres (3) minutos de desatención de la misma (pantalla limpia), protegiendo de esta manera la información importante para la Unidad que reposa en estos equipos, el acceso a las aplicaciones y demás servicios que se tengan desplegados en los mismos*.

S.E. Sin embargo, como se mencionó en el control A.6.1.1 Roles y responsabilidades para la seguridad de información, durante la aplicación de listas de verificación a los usuarios, se evidenciaron equipos desatendidos sin estar bloqueados.

Recomendación: Reforzar la aplicación por parte de los usuarios del principio de que "*Toda sesión de trabajo en los equipos de cómputo o terminales en la Unidad se debe bloquear o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña cuando no estén siendo atendidos*", con el fin de evitar accesos no autorizados a la información de la UAECD.

A.11.2.9. Política de escritorio limpio y pantalla limpia.

Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

S.E. La Unidad tiene documentada la Política de Escritorio y Pantalla Limpios, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. del 29/10/2019, y se observó que, a través de comunicaciones realizadas a través del boletín interno y las pantallas de televisión, se ha hecho énfasis en la apropiación de la política en mención. No obstante, como se indicó en el control A.6.1.1 Roles y responsabilidades para la seguridad de información, durante la aplicación de

listas de verificación a los usuarios, se evidenciaron equipos desatendidos sin estar bloqueados, así mismo se observó acumulación de documentos sobre los escritorios, en especial en la Gerencia Comercial y de Atención al Usuario.

Recomendación: Reforzar la aplicación de la Política de pantalla y escritorio limpios, en cuanto a que escritorio limpio "*se refiere a la protección de la información y de los dispositivos removibles de almacenamiento de información, ubicados en puestos de trabajo (escritorio, oficina, etc.) de accesos no autorizados, pérdida o daño de la información durante y fuera del horario laboral*.", (definición tomada del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información) y que el responsable de velar porque la información se encuentre protegida es el propietario de la información.

6.1.7. Seguridad de las operaciones. (Dominio A.12 NTC-ISO/IEC 27001:2013)

6.1.7.1. A.12.1 Procedimientos operacionales y responsabilidades Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

A.12.1.1. Procedimientos de operación documentados.

Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.

S.E. La UAECD cuenta con quince -15- procedimientos documentados en el Proceso de Provisión y Soporte de Servicios de TI, requeridos para la gestión (provisión, administración, operación, soporte, monitoreo y evaluación) de los servicios, en concordancia con la arquitectura tecnológica de referencia y el catálogo de servicios de TI. Así mismo, dentro del Proceso de Gestión Integral del Riesgo, se tienen documentados seis -6- procedimientos relacionados con el Subsistema de Seguridad y Privacidad de la Información.

A.12.1.2. Gestión de cambios.

Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

S.E. La Unidad tiene documentado el Procedimiento Gestión de Cambios y Liberaciones, código 13-02-PR-31, V.5 del 02-05-2019, asociado al Proceso de Provisión y Soporte de Servicios de TI, cuyo objetivo es "*Asegurar que los cambios sobre los recursos tecnológicos sean notificados, registrados, evaluados, autorizados, priorizados, planificados, ejecutados, probados, documentados, y dispuestos en producción de manera controlada con el fin de reducir incidentes, interrupciones severas, y retrabajo asociados al cambio, en el marco de las mejores prácticas de Information Technology Infraestructure Library – ITIL".*

S.E. También se cuenta con el Procedimiento Gestión del Cambio para la Seguridad y Salud en el Trabajo, código 06-06-PR-05, V.1 del 12/10/2019, asociado al Proceso de Gestión del Talento

Humano Procedimiento, cuyo objetivo es "*Evaluar el impacto sobre la seguridad y salud en el trabajo que puedan generar los cambios internos (nuevos procesos, cambio en los métodos de trabajo, cambios en instalaciones, entre otros).".*

A.12.1.3. Gestión de capacidad.

Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.

S.E. Se observó el Procedimiento Gestión de Capacidad, código 13-02-PR-11, V.3 del 30/10/2018, asociado al Proceso de Provisión y Soporte de Servicios de TI, cuyo objetivo es "*Gestionar las necesidades de los recursos tecnológicos de infraestructura que apoyan o soportan los procesos que componen la cadena de valor de la Unidad.".*

A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación.

Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

S.E. Se evidenció que, en las condiciones especiales de operación del Procedimiento Mantenimiento de Aplicaciones, código 13-02-PR-19, V.3 del 02/01/2018, se indica que "*j) Las actividades del presente procedimiento se realizan en los siguientes ambientes: desarrollo, pruebas y producción. (…) m) En la siguiente tabla, se ilustran las tareas y sus responsables que hacen parte o conforman cada una de las actividades antes mencionadas (Actividades ciclo de vida del desarrollo de software)",* con lo cual se reducen los riesgos de accesos o cambios no autorizados al ambiente de operación de los desarrollos de la Unidad.

6.1.7.2. A.12.2 Protección contra códigos maliciosos. Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

A.12.2.1. Controles contra códigos maliciosos.

Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

S.E. La Unidad cuenta con Antivirus Symantec, firewall, de Fortinet, en el cual se puede parametrizar las funciones de filtrado de red (similar al proxy), IPS (Sistema de detección de intrusos) los cuales son parametrizados para controlar la infección por códigos maliciosos.

6.1.7.3. A.12.3 Copias de respaldo Objetivo: Proteger contra la pérdida de datos.

A.12.3.1. Respaldo de información.

Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

S.E. Se observó que la entidad tiene documentada la Política de Copias de Respaldo y Recuperación, en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, V.6. del 29/10/2019, así como el Procedimiento Copias de Respaldo y Recuperación, código 13-02-PR-32, V.1 del 22/08/2017.

S.E. Se evidenció durante las visitas a las áreas, que en la Subgerencia de Infraestructura Tecnológica hay un profesional designado para la realización de los backups y que se sigue el procedimiento indicado.

S.E. La UAECD cuenta con un centro de datos alternos, ubicado en la ciudad de Cali, como se menciona más adelante en el control A.17.2.1. Disponibilidad de instalaciones de procesamiento de información, que respalda la información de la entidad, con actualización permanente, y le permitiría operar a la Unidad durante una contingencia.

6.1.7.4. A.12.4 Registro y seguimiento Objetivo: Registrar eventos y generar evidencia.

A.12.4.1. Registro de eventos.

Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

S.E. Se cuenta con el Procedimiento Gestión de Eventos, código 13-02-PR-08, V.3 del 25/06/2018, asociado al proceso de Provisión y Soporte de Servicios de TI, cuyo objetivo es "*Realizar el monitoreo, registro de solicitudes de los eventos presentados, el análisis y desempeño de los recursos tecnológicos para gestionar los eventos presentados e identificar oportunidades de mejora en los servicios de TI (...)",* a través del cual se asignan roles y responsabilidades para la gestión de eventos, los cuales son reportados y gestionados a través de la herramienta de mesa de servicios TI.

A.12.4.2. Protección de la información de registro.

Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.

S.E. Con el fin de proteger contra alteración y acceso no autorizado la información de registro, los sistemas y aplicativos de la Unidad cuentan con control de accesos a través de perfiles de

usuarios y asignación de claves, de acuerdo con lo indicado en el Procedimiento Gestión de Accesos, código 13-02-PR-04.

A.12.4.3. Registros del administrador y del operador.

Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.

S.E. Se observa que, en el Procedimiento Gestión de Accesos, código 13-02-PR-04, se establecieron depuraciones periódicas, "*d) Revisiones de las cuentas de usuario privilegiadas asignadas a los administradores de recursos tecnológicos y sus permisos se realizarán semestralmente. (…) Gestor de accesos valida cuentas privilegiadas para continuar o ser depuradas*."

S.E. Igualmente, en el numeral 3.9. Administración de cuentas de usuario, se establece que *(...) Los privilegios de administración sobre los equipos de cómputo deberán ser asignados únicamente a personal de la mesa de servicios de TI, cualquier excepción deberá ser aprobada por el Gestor de Accesos. La cuenta de administración sobre los equipos de cómputo deberá ser custodiada por la Subgerencia de Infraestructura Tecnológica y deberá cambiarse su contraseña cada 3 meses. (...)*

S.E. Se evidenció que las depuraciones son realizadas de acuerdo con lo establecido en el procedimiento.

A.12.4.4. Sincronización de relojes.

Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

S.E. La sincronización de los relojes de los dispositivos de seguridad informática y sistemas de procesamiento de información se hace a través de un servidor NTP.

6.1.7.5. A.12.5 Control de software operacional Objetivo: Asegurar la integridad de los sistemas operacionales.

A.12.5.1. Instalación de software en sistemas operativos.

Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.

S.E. La entidad cuenta con la Política de Instalación y Uso de Software, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02. Durante el seguimiento realizado para el informe de Derechos de Autor Software, durante el mes de octubre de 2019, se realizaron pruebas para verificar las

restricciones de instalación de software a 64 equipos de escritorio, de lo cual se verificó el cumplimiento de los lineamientos dados en la política.

6.1.7.6. A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

A.12.6.1. Gestión de las vulnerabilidades técnicas.

Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

S.E. En entrevista a la Oficial de Seguridad, se observó la propuesta para el procedimiento de gestión de vulnerabilidades técnicas.

Recomendación: Revisar la propuesta para el procedimiento de gestión de vulnerabilidades técnicas, y de considerarlo pertinente, aprobar y socializar la propuesta. Actualizar la información en la Declaración de Aplicabilidad.

A.12.6.2. Restricciones sobre la instalación de software.

Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

S.E. Como se mencionó en el control A.12.5.1. Instalación de software en sistemas operativos, la entidad tiene implementados los controles necesarios para la instalación de software por parte de los usuarios.

6.1.8. Seguridad de las comunicaciones. (Dominio A.13 NTC-ISO/IEC 27001:2013)

6.1.8.1. A.13.1 Gestión de la seguridad de las redes. Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

A.13.1.1. Controles de redes.

Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

S.E. En entrevista con la Oficial de Seguridad, indicó que se utilizan certificados digitales para el transporte de información de red externa por servicios web.

A.13.1.2. Seguridad de los servicios de red.

Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

S.E. En entrevista con la Oficial de Seguridad, se informó que la entidad cuenta con una Red Privada Virtual (VPN por sus siglas en inglés Virtual Private Network), LDAP (Lightweight Directory Access Protocol, en español Protocolo Ligero/Simplificado de Acceso a Directorios) que es un protocolo para acceder y mantener servicios de información de directorio distribuidos a través de una red de protocolo de Internet, firewall y routers parametrizados para tener altos niveles de seguridad y servicio de la infraestructura de la entidad.

S.E. El proceso de Provisión y Soporte de Servicios de TI tiene documentado el indicador NIVEL DE DISPONIBILIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA, cuya meta es del 95% y que durante el 2019 ha presentado mediciones trimestrales del 99,07%, 99,24% y 99,13%.

A.13.1.3. Separación en las redes.

Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

S.E. Para la aplicación de este control, la entidad ha definido niveles para el acceso a los servicios de red, básico intermedio y avanzado, así mismo se tienen controles definidos e implementados a través del Proceso de Control de Accesos y se cuenta con dispositivos de seguridad informática: firewall, VLan, routers, switch, entre otros.

6.1.8.2. A.13.2. Transferencia de información. Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

A.13.2.1. Políticas y procedimientos de transferencia de información.

Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

S.E. Se evidenció que la entidad cuenta con la Política de transferencia de información, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02.

S.E. Como se indicó en el control A.6.1.1 Roles y responsabilidades para la seguridad de información, los usuarios no tienen claridad en cuál información transfieren, ni cómo debe hacerse, ni los lineamientos para hacerlo.

S.E. Igualmente, como se mencionó en el control A.7.2.3 Proceso disciplinario, en cuanto a los documentos relacionados con investigaciones disciplinarias, no se están siguiendo los

lineamientos establecidos en la política para transferencia de información de carácter clasificada o reservada, incumpliendo con la normatividad vigente para el control disciplinario y el debido proceso.

S.E. Para el caso de solicitudes de **transferencia de información provenientes de entidades externas**, que tiene a cargo la Gerencia Comercial y de Atención al Usuario - GCAU, el día 24 de octubre de 2019, se aplicó una lista de verificación a la Profesional de la gerencia, encargada de recibir y dar trámite a las solicitudes de entidades externas para acceder a la información misional de la UAECD a través de los aplicativos propios de la entidad. En este sentido, se evidenció que la Unidad tiene documentado el Subproceso Gestión Comercial, código 05-SP-01, V.5 del 12/04/2019, que dentro una de sus políticas de operación establece "*La Gerencia Comercial y de Atención al Usuario será la encargada de recepcionar las solicitudes de las entidades interesadas en acceder a la información puesta a disposición por la UAECD y gestionará ante la Gerencia de Tecnología la asignación de perfiles, claves y contraseñas con el fin de acceder a la información*.".

Así mismo, se observó el Procedimiento Acceso y Disposición de Información, código 05-01-PR-08, V.4 del 14/06/2019, que tiene por objetivo establecer las actividades necesarias para que las entidades de la administración pública accedan de forma segura a la información física, jurídica y económica de los bienes inmuebles de la ciudad de Bogotá, que la Unidad tiene dentro sus activos de información, como parte de este procedimiento se tienen los formatos: Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de la Unidad Administrativa Especial de Catastro Distrital - UAECD, código 06-01-FR-40, el Acta de Autorización de Consulta de Información Predial de la Unidad Administrativa Especial de Catastro Distrital – UAECD, código 05-01-FR-18 y el Registro de Atención de Requerimientos de Acceso a la Información, código 05-01-FR-16.

Con la Profesional de la GCAU se verificaron cada una de las actividades descritas en el procedimiento, se observó el diligenciamiento de los formatos requeridos (para lo cual se tomaron 2 entidades como muestra: Contraloría General de la República y Fiscalía General de la Nación), así como el diligenciamiento del registro de atención de requerimientos, de lo cual se evidenció que se está dando cumplimiento a los lineamientos descritos tanto en la Política de Transferencia de Información como en los del Procedimiento Acceso y Disposición de Información.

Recomendación: Modificar el numeral 2.7.2. Alcance, del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, teniendo en cuenta que el control de seguridad "*Políticas y procedimientos de transferencia de información*", corresponde al control A.13.2.1. y no al A.13.2.11. Atender las recomendaciones y hallazgos registrados en el presente informe para los controles A.6.1.1 Roles y responsabilidades para la seguridad de información y A.7.2.3 Proceso disciplinario.

A.13.2.2. Acuerdos sobre transferencia de información.

Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.

S.E. Como se mencionó en el ítem anterior, para la transferencia de información con entidades externas, se cuenta con los formatos Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología de la Unidad Administrativa Especial de Catastro Distrital - UAECD, código 06-01-FR-40, el Acta de Autorización de Consulta de Información Predial de la Unidad Administrativa Especial de Catastro Distrital – UAECD, código 05-01-FR-18 , que son firmados por las entidades externas antes de tener acceso a la información predial que captura, procesa y dispone de la Unidad.

A.13.2.3. Mensajería electrónica.

Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.

S.E. Para proteger la información incluida en la mensajería electrónica, se tiene parametrizado el antivirus y los controles de seguridad de Microsoft que se adquirieron con la solución Office 365, con reglas que permiten bloquear amenazas procedentes de la red y evitar la recepción de correo no deseado o dañino, tales como antispam, listas negras de direcciones IP, cuentas de correo o contenido.

A.13.2.4. Acuerdos de confidencialidad o de no divulgación.

Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

S.E. Aplica la situación evidenciada en el control anterior, A.13.2.2. Acuerdos sobre transferencia de información.

Recomendación: Actualizar la información en la Declaración de Aplicabilidad, por cuanto no se tiene un formato de "Acuerdo de Confidencialidad", e incluir el formato Acta de Autorización, código 05-01-FR-18.

6.1.8. Adquisición, desarrollo y mantenimientos de sistemas. (Dominio A.14 NTC-ISO/IEC 27001:2013)

6.1.8.1. A.14.1. Requisitos de seguridad de los sistemas de información. Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

A.14.1.1. Análisis y especificación de requisitos de seguridad de la información.

Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

S.E. Se observó que la Unidad cuenta con el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, V.1 del 20/09/2018, asociado al Proceso de Provisión y Soporte de Servicios de TI, en el que, entre otros temas, se menciona "*3.1.2.1. Evaluar viabilidad del mantenimiento, analizar requerimientos y diseñar la solución de software: Los requisitos relacionados con seguridad de la información para nuevos sistemas de información o para mejoras a los ya existentes (...)".*

S.E. Así mismo, se tiene documentado el Procedimiento Mantenimiento de Aplicaciones, código 13-02-PR-19, V.3 del 02/01/2018 y el formato Evaluación Viabilidad del Mantenimiento, código 13-02-FR-36, V.2 del 14/12/2017, que incluyen los requisitos de seguridad de la información para los desarrollos nuevos de software y las modificaciones de los ya existentes, el cual es aplicado por los líderes funcionales y técnicos de cada uno de los aplicativos que tiene la Unidad.

A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. **Control**: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificaciones no autorizadas y A.14.1.3. Protección de transacciones de los servicios de las aplicaciones. **Control**: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada

S.E. En entrevista con la Oficial de Seguridad, para los dos controles en mención, se informó que la entidad cuenta con certificados digitales para los servicios web, que permiten la identificación exclusiva de la Unidad, con lo cual se protege la información y las transacciones que son transmitidas a través de redes públicas.

6.1.8.2. A.14.2. Seguridad en los procesos de desarrollo y soporte. Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

A.14.2.1. Política de desarrollo seguro.

Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.

S.E. La Unidad cuenta con el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, V.1 del 20/09/2018 y con el

Procedimiento Mantenimiento de Aplicaciones, asociados al Proceso de Provisión y Soporte de Servicios de TI, que se aplican para el desarrollo de aplicaciones in situ.

A.14.2.2. Procedimientos de control de cambios en sistemas.

Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.

S.E. Se evidenció la documentación de los procedimientos: Mantenimiento de Aplicaciones, código 13-02-PR-19, V.3 del 02/01/2018, Gestión de Problemas, código 13-02-PR-09, V.3 del 05/09/2018, Gestión de la Infraestructura Tecnológica, código 13-02-PR-36, V.2 del 25/06/2018 y Gestión de Configuración, código 13-02-PR-13, V.2 del 09/06/2017, asociados al Proceso Provisión y Soporte de Servicios TI, todos ellos establecen lineamientos o actividades que buscan controlar los cambios que se producen tanto en el software como en el hardware que componen y soportan la tecnología de la Unidad.

Recomendación: Actualizar la información en la Declaración de Aplicabilidad, por cuanto el Procedimiento Gestión del Catálogo de Servicios TI se encuentra obsoleto desde el 03/05/2019.

A.14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.

Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.

S.E. A través del Procedimiento Gestión de Cambios y Liberaciones, código 13-02-PR-31, V.5 del 02/05/2019, se establecen los lineamientos para ejecutar, probar y documentar los cambios sobre los recursos tecnológicos de la Unidad, y se asignan los roles o grupos operativos encargados de llevar a cabo la gestión de cambios y liberaciones, para asegurar que los mismos han sido probados en un entorno de prueba, evaluados y mitigados sus impactos, están alineados con la arquitectura tecnológica de la Unidad, antes de salir a producción.

A.14.2.4. Restricciones en los cambios a los paquetes de software.

Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

S.E. Para éste control también aplica el Procedimiento Gestión de Cambios y Liberaciones, código 13-02-PR-31, puesto que da los lineamientos necesarios para identificar, controlar, dar seguimiento y auditar los requerimiento de cambio de TI, de los cuales se lleva trazabilidad a través de la mesa de servicios de TI, desde la solicitud, con el formato Solicitud de Cambio o Actualización de Aplicaciones, código 13-02-FR-14, V.2, hasta su paso a producción con el formato Acta Paso a Producción - Solicitud de Cambio o Actualización de Aplicaciones, código 13-02-FR-15, V.2.

A.14.2.5. Principios de construcción de sistemas seguros.

Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

S.E. Como se mencionó en el control A.14.2.1. Política de desarrollo seguro, la Unidad cuenta con el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, V.1 del 20/09/2018 y con el Procedimiento Mantenimiento de Aplicaciones, asociados al Proceso de Provisión y Soporte de Servicios de TI, que se aplican para el desarrollo de aplicaciones in situ.

A.14.2.6. Ambiente de desarrollo seguro.

Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

S.E. Se observó que, a través de los controles para el proceso de ciclo de vida del desarrollo de software, establecidos en el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, se busca garantizar que los ambientes de desarrollo, pruebas y producción se configuren de forma segura, teniendo en cuenta los controles de seguridad y privacidad de la información asociados a la premisa "*Los controles se implantan proporcionalmente de acuerdo a la comodidad de uso y la protección de la información.".* Así mismo, en el documento en mención, se observó la tabla "*Controles de seguridad y privacidad de la información a ser aplicados sobre los ambientes que soportan el ciclo de vida de desarrollo de software*.

A.14.2.7. Desarrollo contratado externamente.

Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

S.E. Se evidenció el contrato 234-2018 con el CONSORCIO CATASTRO S&S, cuyo objeto es "*Prestar los servicios de implementación de componentes de software para la UAECD.",* con fecha de finalización 31 de diciembre de 2019, el cual cuenta con las cláusulas: "*15) OBLIGACIONES DEL SUPERVISOR: 15.1) Hacer seguimiento a la ejecución del contrato, en los términos previstos en los estudios previos, en el pliego de condiciones, sus adendas en caso que las hubiere, el anexo técnico y demás documentos que hacen parte integral del proceso y con lo ofrecido en la propuesta presentada a través de la cláusula*." y "*16) COMITÉ TÉCNICO. La UAECD conformará un comité técnico para la identificación de las necesidades de software, la coordinación de la ejecución de las pruebas y la aprobación a entera satisfacción de las mismas. El Comité Técnico será regulado por la entidad en cuanto a su conformación y funciones y demás aspectos que se requieran para su normal*

funcionamiento.", a través de las cuales se realiza el seguimiento de las actividades desarrolladas por el contratista durante la ejecución de sus obligaciones.

A.14.2.8. Pruebas de seguridad de sistemas.

Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

S.E. En las condiciones especiales de operación del Procedimiento Mantenimiento de Aplicaciones, código 13-02-PR-19, V.3 del 02/01/2018, se menciona que uno de los ambientes a desarrollar es el de *Pruebas*, donde se planifican y ejecutan pruebas y, en el ítem m) a través de una tabla, se muestran las actividades del procedimiento y sus responsables, dentro de las cuales se observaron: "*Ejecutar procedimiento pruebas y certificación de servicios SOA",* "*Planificar y ejecutar pruebas*", cada una de ellas con sus respectivas tareas.

S.E. Así mismo, en el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, se evidenció el ítem 3.1. Principios de Construcción de Sistemas Seguros, en el cual se relacionan los controles de seguridad y privacidad a implementar asociados a los principios de construcción de sistemas seguros, de acuerdo con los lineamientos establecidos en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información.

A.14.2.9. Prueba de aceptación de sistemas.

Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.

S.E. En el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, se observó la Tabla 4 "*Controles de seguridad y privacidad de la información a ser aplicados, con base en las propiedades fundamentales de seguridad de la información*" *(...)* que menciona en el control de "*Auditoría",* entre otros puntos: *"f. Las pruebas de aceptación para requisitos de seguridad de la información incluyen las pruebas de vulnerabilidades cuando sean requeridas, se realizan teniendo en cuenta que: (...)".*

S.E. En el Procedimiento Mantenimiento de Aplicaciones, código 13-02-PR-19, se especifica la elaboración de pruebas antes y después de que un nuevo sistema o una actualización salga a producción, se establece la obligatoriedad de elaborar la matriz de pruebas y el guion de pruebas, y la ejecución de las actividades de pruebas y su adecuada documentación.

6.1.8.3. A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas.

A.14.3.1. Protección de datos de prueba

Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente

S.E. Se evidenció que, en el Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro, código 13-02-DT-01, Tabla 4 "*Controles de seguridad y privacidad de la información a ser aplicados, con base en las propiedades fundamentales de seguridad de la información*", se dan los lineamientos para los controles de las pruebas de un sistema de información nuevo o la mejora de uno ya existente, entre otros: "*Se aplican técnicas de cifrado para minimizar la exposición para datos personales sensibles", "Haciendo uso de herramientas descritas en el Instructivo de alistamiento y entrega de equipos de escritorio, código 13-02-IN-06, se realiza un borrado seguro de la información cuando se finaliza el uso de datos reales a los ambientes de desarrollo y pruebas"*

S.E. En entrevista con la Oficial de Seguridad, se observó el documento "Informe de revisión a protección de datos de pruebas", realizado en julio de 2019 por uno de los profesionales del equipo de Seguridad de la Información.

6.1.9. Relación con los proveedores. (Dominio A.15 NTC-ISO/IEC 27001:2013)

6.1.9.1. A.15.1 Seguridad de la información en las relaciones con los proveedores. Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

A.15.1.1. Política de seguridad de la información para las relaciones con proveedores.

Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.

S.E. Se evidenció la Política para la Relación con Proveedores en la Etapa Precontractual y Contratista en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, en la cual se establecen los lineamientos que definen las reglas para proteger la confidencialidad, integridad y disponibilidad de la información de la Unidad, la cual es accedida por un proveedor en la etapa precontractual y/o contratista.

A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.

Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

S.E. La entidad tiene establecido el formato Anexo Técnico, código 11-01-FR-16, que se debe diligenciar y anexar a los estudios previos de cada contratación, el cual contiene la casilla "Especificaciones Técnicas", donde se deben describir puntualmente los requerimientos técnicos que se necesitan para el desarrollo del contrato: medidas, espacios, niveles de servicios, tipo de mantenimiento, soporte en sitio, recurso humano, requerimientos de seguridad de la información, etc. Por otra parte, se tiene establecido el Compromiso de confidencialidad y uso de la información de la UAECD, el cual debe ser firmado por todos los

contratistas antes de iniciar la ejecución del contrato, además de las cláusulas de confidencialidad que se dejan estipuladas dentro de las obligaciones contractuales.

S.E. Con el fin de verificar el cumplimiento de los lineamientos antes mencionado, se revisaron 8 contratos vigentes al momento de la presente auditoría, que tienen acceso a información de la Unidad, los cuales se muestran a continuación:

Tabla 2: Revisión contratos con personas jurídicas

Tipo Contrato	No Contrato	Contratista	Objeto	Observación OCI
Prestación de Servicios de Vigilancia	202-2018	U.T. Zona Sencacol 2018	El contratista se obliga a prestar los servicios de vigilancia y seguridad privada, para la permanente y adecuada protección de los funcionarios, contratistas, visitantes, contribuyentes y usuarios de la entidad y los bienes muebles e inmuebles objeto de la contratación.	Proceso llevado a cabo por la Secretaría de Hacienda, no se observan cláusulas de confidencialidad.
Compraventa	209-2018	MSL Distribuciones & Cía. S.A.S.	Prestación del servicio de soporte, mantenimiento y la ampliación del número de licencias de clientes para el software de mesa de servicio.	El acuerdo de confidencialidad es un anexo publicado en Secop junto con los pliegos, pero no se relaciona en los mismos ni en los estudios previos, ni se evidencia el documento firmado. No se observan compromisos de confidencialidad del personal que labora en las instalaciones de la Unidad.
Prestación de Servicios	213-2018	Origen Soluciones Informáticas y de Software SAS.	Servicio integral de mantenimiento con bolsa de repuestos, y soporte técnico para equipos de cómputo de escritorio y periféricos	El acuerdo de confidencialidad es un anexo publicado en Secop junto con los pliegos, pero no se relaciona en los mismos ni en los estudios previos, ni se evidencia el documento firmado. No se observan compromisos de confidencialidad del personal que labora en las instalaciones de la Unidad.
Prestación de Servicios	229-2018	Servicios Postales Nacionales	Prestar servicios de a) servicios postales, b) Mensajería expresa, c) Envío de paquetes, documentos y demás envíos en todas las modalidades del servicio a nivel urbano, nacional e internacional, d) impresión fija y variable de actos administrativos masivos, comunicaciones y avisos y e) La notificación electrónica de actos administrativos; incluyendo el personal requerido para atender la operación propia de la mensajería interna y externa.	A la fecha de la auditoría, se observó que hay 15 personas laborando en la Unidad, sin embargo, solamente se evidenció la Carta de Compromiso de confidencialidad de 7 de ellos.

Tipo Contrato	No Contrato	Contratista	Objeto	Observación OCI
Prestación de Servicios	213-2019	MEDICAL PROTECTION LTDA SALUD OCUPACIONAL	Prestar los servicios para la realización de evaluaciones médicas ocupacionales a los servidores de la UAECD dentro del Sistema de Gestión de la Seguridad y Salud en el Trabajo, de conformidad con las normas vigentes en la materia	El acuerdo de confidencialidad es un anexo publicado en Secop junto con los pliegos, y se menciona en los estudios previos, sin embargo, el documento **no se evidencia firmado, ni física ni digitalmente**. TITULO I, DEL CONTRATO A CELEBRAR, numeral *9. Confidencialidad de la información El CONTRATISTA guardará confidencialidad sobre la información que obtenga de la UAECD en desarrollo del objeto contractual. El contratista deberá suscribir el Compromiso de confidencialidad que establezca la entidad y garantizará que su personal mantenga confidencial la información de la UAECD a la que tenga acceso*.
Prestación de Servicios	254-2019	UT Custodia 2019	Prestar los servicios integrales en la modalidad de outsourcing para la custodia, consulta, préstamo y administración del archivo central de la UAECD.	Se evidenció acuerdo de confidencialidad firmado. TITULO I, DEL CONTRATO A CELEBRAR, numeral 10. Confidencialidad de la información El CONTRATISTA guardará confidencialidad sobre la información que obtenga de la UAECD en desarrollo del objeto contractual. El contratista deberá suscribir el Compromiso de confidencialidad que establezca la entidad y garantizará que su personal mantenga confidencial la información de la UAECD a la que tenga acceso.
Obra	261-2019	ALTACIVILES SAS	Prestar el servicio de mantenimiento locativo y adecuaciones de las instalaciones de la UAECD, incluido el suministro de mano de obra y materiales	Se evidenció acuerdo de confidencialidad firmado. 6 CAPÍTULO SEXTO - DEL CONTRATO A CELEBRAR. 6.11 Confidencialidad de la información. El CONTRATISTA guardará confidencialidad sobre la información que obtenga de la UAECD en desarrollo del objeto contractual. El contratista deberá suscribir el Acuerdo de confidencialidad que establezca la entidad y garantizará que su personal mantenga confidencial la información de la UAECD a la que tenga acceso.
Compraventa	304-2019	SOFTWARE AUTOMATION AND TECHNOLOGY LTDA-SAUTECH LTDA.	Adquirir el sistema de control de accesos para las áreas de la UAECD.	Se evidenció acuerdo de confidencialidad firmado. Numeral 10 de pliegos de condiciones: 10. Confidencialidad de la información. (…). El contratista deberá suscribir el Acuerdo de confidencialidad que establezca la entidad y garantizará que su personal mantenga confidencial la información de la UAECD a la que tenga acceso.

Elaboración propia del auditor. Información tomada del SECOP y expedientes contractuales.

Hallazgo:
(OM) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció la desactualización de los formatos de Estudios y Documentos Previos y, los Procedimientos para cada una de las modalidades de contratación de la Unidad, por cuanto en ellos se hace mención del "*Acuerdo de confidencialidad*", el cual no existe en los documentos del Sistema de Gestión Integral de la Unidad, lo que podría conllevar confusión al momento de llevar a cabo el procedimiento en mención.

(OM) A partir de la auditoría al SGSI de la UAECD 2019, se observó que los formatos de Estudios y Documentos Previos de las diferentes modalidades de contratación, no contienen las mismas obligaciones o lineamientos (análisis de riesgos) con respecto a la seguridad de la información; así mismo, al momento de ser diligenciados son modificados y se eliminan parcialmente obligaciones generales del contratista, relacionadas con la confidencialidad y seguridad de la información de la UAECD, lo que contraviene lo establecido en los documentos en sí y que hacen parte del Procedimiento de cada una de las modalidades de contratación aprobadas por la Entidad. Eliminar y/o modificar las obligaciones del contratista, antes mencionadas, podría causar la materialización de los riesgos relacionados con el manejo de la información por parte de terceros externos.

(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció que hay contratos con personas jurídicas que no tienen el acuerdo de confidencialidad suscrito y firmado, ni los acuerdos con los terceros que realicen labores en la entidad, como se establece en los formatos de Estudios y Documentos Previos de las diferentes modalidades de contratación: "*Suscribir el acuerdo de confidencialidad de la información con la Unidad*" y "*Suscribir el acuerdo de confidencialidad de la información con los terceros que tengan relación con la ejecución del objeto del contrato*", lo que podría generar pérdida o manipulación de información, y en general la materialización de los riesgos relacionados con el SGSI.

A.15.1.3. Cadena de suministro de tecnología de información y comunicación.

Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

S.E. En los formatos de Estudios y Documentos Previos de las modalidades de selección contratación directa, mínima cuantía, subasta inversa, licitación, contienen *Análisis del sector*, en el que se indican, entre otros puntos, que el área de origen hace constar que durante la etapa de planeación realizó el análisis necesario para conocer los riesgos asociados a la seguridad de la información. Se evidenció que el formato de estudios previos para la modalidad de selección de menor cuantía no especifica el análisis de riesgos relacionados con la seguridad de la información. Así mismo, se tiene el formato Matriz de Asignación de Riesgos Previsibles, código 11-01-FR-13.

S.E. En la revisión efectuada a los contratos relacionados en la Tabla 2 del presente informe, no se evidenció que en el ítem Análisis del Sector o en la Matriz de Asignación de Riesgos Previsibles se hayan incluido riesgos asociados a la seguridad de la información.

Recomendación: Realizar una capacitación liderada por la Oficial de Seguridad, dirigida al personal que elabora los estudios previos en cada dependencia de la Unidad, con el fin de dar indicaciones sobre los posibles riesgos de información que podrían tener en sus procesos contractuales y contratos, y así construir una matriz de asignación de riesgos más completa.

Hallazgo
(OM) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció que el formato de Estudios y Documentos Previos Modalidad de Selección Abreviada de Menor Cuantía, código 11-01-FR-08, en el ítem Análisis de Sector, no señala el análisis correspondiente a los riesgos asociados a la seguridad de la información, como se observa en los otros formatos de estudios previos de las demás modalidades de contratación, lo que podría generar la materialización de amenazas y poner en riesgo la prestación del servicio contratado.

6.1.9.2. A.15.2 Gestión de la prestación de servicios con los proveedores Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

A.15.2.1. Seguimiento y revisión de los servicios de los proveedores.

Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

S.E. Se observó que la entidad cuenta con el Documento Técnico Manual de Contratación, código 11-02-DT-01, V.2 del 29/12/2017, y en el capítulo 6, da los lineamientos para la "*Supervisión e Interventoría"* de los contratos suscritos por la Unidad. Así mismo, se tiene el Procedimiento Ejecución y Supervisión de Contratos, código 11-02-PR-02, V.4 del 26/06/2019, los dos asociados al Proceso de Gestión Contractual.

S.E. Por otra parte, la Oficina de Control Interno, realiza 2 auditorías en cada vigencia con el fin de verificar la ejecución presupuestal, el plan de contratación, el Comité de Contratación y la contratación en sus fases de planeación, selección, contratación, ejecución, a partir del cual se generan las oportunidades de mejora o acciones correctivas a que haya lugar.

A.15.2.2. Gestión de cambios en los servicios de proveedores.

Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

S.E. No se evidenció un lineamiento que contemple la gestión de cambios en los servicios con los proveedores de la Unidad.

Recomendación: Revisar la pertinencia de trabajar en lineamientos sobre gestión de cambios en los servicios con proveedores de la Unidad, en el plan de trabajo de la Oficial de Seguridad de la

Información, con el fin de que, al momento de presentarse cambios, se realice con el mínimo de interrupciones en la prestación de los servicios.

6.1.10. Gestión de incidentes de seguridad de la información. (Dominio A.16 NTC-ISO/IEC 27001:2013)

6.1.10.1. A.16.1. Gestión de incidentes y mejoras en la seguridad de la información. Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

A.16.1.1. Responsabilidad y procedimientos.

Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

S.E. Se observó que la Unidad tiene documentados los procedimientos: Gestión de Incidentes, código 13-02-PR-03, V.3 del 12/08/2019 y Gestión de Eventos, código 13-02-PR-08, V.3 del 25/06/2018 y el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, en el cual, se menciona en repetidas ocasiones la obligación de los funcionarios, contratistas y terceros de reportar los incidentes de seguridad de la información y las responsabilidades de los diferentes roles frente al tema.

A.16.1.2. Reporte de eventos de seguridad de la información. **Control**: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible y A.16.1.3. Reporte de debilidades de seguridad de la información. **Control**: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

S.E. Como se mencionó en el punto anterior, la entidad tiene documentados los Procedimientos Gestión de Eventos, código 13-02-PR-08 y Gestión de Incidentes, código 13-02-PR-03, en los que se indica que el reporte de los eventos o incidentes debe realizarse a través de la mesa de servicios TI. Así mismo, en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, ítem 2.6.3. Todas las Gerencias, Subgerencias y Oficinas de la UACED, se indica que "*b) Todo requerimiento, incidente, problema o cambio relacionado con la seguridad de la información del a UAECD debe ser reportado y tramitado por la herramienta tecnológica de apoyo a la mesa de servicios de TI, único medio válido y autorizado para estos fines."*

S.E. Se evidenció que, como se indicó en el control A.6.1.1. Roles y responsabilidades para la seguridad de información, menos del 50% de los usuarios entrevistados conoce el procedimiento y su aplicación.

A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.

S.E. En cuanto a los eventos de seguridad (amenaza de incidente de seguridad de la información), se observó que a través del Procedimiento Gestión de Incidentes de Seguridad de la Información, código 02-02-PR-01, actividad 1, *Ejecutar actividades preestablecidas para la atención del incidente*, se debe evaluar el tipo de evento/incidente, evaluar si tiene un plan de manejo definido, la severidad y generar un plan de trabajo para la atención del incidente de seguridad o privacidad de la información.

A.16.1.5. Respuesta a incidentes de seguridad de la información.

Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

S.E. Se evidenció que la actividad 9. Resolver incidente, del Procedimiento Gestión de Incidentes, código 13-02-PR-03, señala que se debe resolver el incidente en la herramienta tecnológica de apoyo a la mesa de servicios de TI, documentado las acciones realizadas que solucionaron el incidente, lo cual es notificado a través de correo electrónico al usuario que registró la mesa de servicios reportando el incidente.

A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.

Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

S.E. En entrevista con la Oficial de Seguridad, se evidenció que, dependiendo del tipo de incidente, se toman las medidas requeridas para que éste no se vuelva a presentar: implementando controles, modificando procedimientos, entre otros.

A.16.1.7. Recolección de evidencia.

Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

S.E. Se observó que, en los Procedimientos Gestión de Eventos, código 13-02-PR-08 y Gestión de Incidentes, código 13-02-PR-03, es requisito para la gestión de estos, documentar las acciones realizadas para resolver el evento o incidente registrado, y dicha documentación es guardada anexa al registro que se lleva a través de la mesa de servicios de TI.

S.E. En entrevista con la Oficial de Seguridad se verificaron los incidentes reportados en el mes de septiembre de 2019, los registros realizados en la mesa de servicios de TI, su trazabilidad en

las acciones realizadas para su resolución, las evidencias aportadas y la respuesta dada a la persona que las reportó.

6.1.11. Aspectos de seguridad de la información de la gestión de continuidad de negocio. (Dominio A.17 NTC-ISO/IEC 27001:2013)

6.1.11.1. A.17.1 Continuidad de seguridad de la información. Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

A.17.1.1. Planificación de la continuidad de la seguridad de la información.

Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

S.E. Se evidenció que la UAECD cuanta con planes de continuidad del negocio –BCP-, del Subsistema de Gestión de Continuidad del Negocio – SGCN- actualizados a noviembre de 2018 y se encuentran publicados en la intranet en la ruta http://intranet.catastrobogota.gov.co/?q=es/node/3019.

Recomendación: Se deben revisar y actualizar los documentos del Subsistema de Gestión Continuidad del Negocio, ya que se observa personal no se encuentra actualmente laborando en la Unidad o que está en dependencias o procesos diferentes.

A.17.1.2. Implementación de la continuidad de la seguridad de la información.

Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

S.E. Se observó que desde el año 2013 se encuentra en implementación el Subsistema de Gestión de Continuidad del Negocio - SGCN, y a través del contrato de consultoría 191 de 2018, el Consorcio Mnemo, entregó en junio de 2018: 34 Análisis del Impacto al Negocio correspondientes a los 34 subprocesos de la Unidad, 15 Análisis de Riesgos (RA) correspondientes a los 15 procesos de la Entidad y un Plan de Recuperación Ante Desastres (DRP), los cuales se encuentran publicados en el enlace de la intranet http://intranet.catastrobogota.gov.co/?q=es/node/3019, como se mencionó anteriormente.

S.E. De acuerdo con el plan de trabajo 2019, del Oficial de Continuidad del Negocio, se han realizado campañas de sensibilización a los servidores de la Unidad con respecto al subsistema, sin embargo, como se mencionó en el control A.6.1.1. Roles y responsabilidades para la seguridad de información, el 70% de los usuarios entrevistados desconoce los procesos del Subsistema de Gestión de Continuidad del Negocio en el cual está involucrada al área a la que pertenecen.

A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

S.E. De acuerdo con el plan de continuidad del negocio y el plan de trabajo del Oficial de Continuidad del Negocio, evidenciado durante el seguimiento al Subsistema de Gestión de Continuidad del Negocio del mes de agosto de 2019, durante la vigencia 2019 se han realizado 2 pruebas al Subsistema, una en el mes de febrero y otra en junio, las cuales se tienen fueron debidamente planeadas, ejecutadas y documentadas.

6.1.11.2. A.17.2 Redundancias. Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

A.17.2.1. Disponibilidad de instalaciones de procesamiento de información.

Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

S.E. Se observó que la UAECD tiene vigente el contrato interadministrativo 211-2018 con la Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., cuyo objeto es "*Prestación del servicio de contingencia y canales de comunicación e Internet para los procesos informáticos que soportan la operación de la UAECD"*, el cual finaliza el 31/12/2019, y a través del cual la Unidad adquirió los servicios de un centro de datos alterno ubicado en la ciudad de Cali, que respalda la información de la entidad, con actualización permanente, y le permitiría operar a la entidad durante una contingencia.

S.E. También se evidenció la realización de pruebas al centro de datos alterno, una enfocada a probar el plan de recuperación ante desastres (DRP) y otro al plan de continuidad del negocio (BCP), en los meses de febrero y junio respectivamente, y se tiene programado otro ejercicio para el mes de diciembre de 2019. Así mismo, se observan los informes de disponibilidad mensuales, remitidos por la ETB al supervisor del contrato.

6.1.12. Cumplimiento. (Dominio A.18 NTC-ISO/IEC 27001:2013)

6.1.12.1. A.18.1 Cumplimiento de requisitos legales y contractuales. Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

A.18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales.

Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización

S.E. Se evidenció que la entidad cuenta con un normograma, publicado en la herramienta ISODOC, donde se publican las normas de carácter constitucional, legal, reglamentario y de autorregulación, que son de interés para la entidad y que es de permanente consulta de todos los servidores de la Unidad. Igualmente, se tiene documentada la cadena de valor de la entidad: 15 procesos divididos en Procesos Estratégicos, Misionales, de Apoyo y de Evaluación y Control, cada uno de ellos con su respectiva caracterización, subprocesos y procedimientos, y demás lineamientos que conforman el Sistema de Gestión Integral.

A.18.1.2 Derechos de propiedad. Intelectual.

Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

S.E. Se evidenció que la entidad cuenta con la Política de Instalación y Uso de Software, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, que da los lineamientos para el uso de software licenciado cobijado por derechos de autor, así mismo, dentro de los principios de la Política de Uso Aceptable se menciona "*Se deben identificar e implementar controles que apoyen el cumplimiento de la normatividad Colombiana vigente con relación a la seguridad y privacidad de la información, como es el caso de la Ley 1915 de 2018 "Por la cual se modifica la Ley 23 De 1982 y se establecen otras disposiciones en materia de Derecho de Autor y Derechos Conexos*".

S.E. Igualmente, la Oficina de Control Interno, elabora anualmente un informe sobre derechos de autor de software; el último se realizó con corte a octubre de 2019.

A.18.1.3. Protección de registros.

Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

S.E. Como se ha indicado en varios de los controles de la Declaración de Aplicabilidad, revisados a través de la auditoría, la entidad tiene implementado mecanismos para la protección de registros digitales, tales como: VPN, firewall, routers, antivirus, bloqueo de páginas, bloqueo de puestos USB, restricción a unidades de CD, DVD, controles de acceso a servicios de red y aplicativos, entre otros.

S.E. Por otra parte, para la protección de archivos físicos, la Unidad cuenta con el Programa de Gestión Documental y se encuentra en proceso de elaboración del Programa de Conservación Documental, así mismo, se evidencian instrumentos para la gestión de la información como: Tablas de Retención Documental –TRD-, Cuadros de Caracterización Documental, - CCD y Registros de Activos de información.

S.E. La entidad cuenta con el Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06.

S.E. Contractualmente, la UAECD tiene implementado el formato de Compromiso de Confidencialidad y cláusulas contractuales en pro de la protección de la información que se captura, integra y dispone en la entidad.

S.E. Se indagó con el encargado del sistema de protección contra incendio de las instalaciones, el cual pertenece a la Secretarita Distrital de Hacienda, e indicó que los detectores de humo no están en funcionamiento, éstos fueron instalados hace aproximadamente 5 meses y se espera realizar pruebas en el mes de noviembre de 2019 para su entrega final.

S.E. Finalmente, como parte de la verificación a la protección de los archivos físicos de la UAECD, y en general de las instalaciones, a través de correo electrónico del 22/10/2019 se solicitó a la Subgerencia Administrativa y Financiera un listado de personas que tienen ingreso a las áreas seguras de la entidad y un registro de ingreso del último mes a las zonas antes mencionadas. Con fecha 30/10/2019 se recibió respuesta al correo en mención, y junto con el equipo auditor, el día 06 de noviembre, se procedió a la verificación de los 15 archivos de gestión distribuidos en los pisos 2, 11 y 12 de entidad, encontrando lo siguiente:

- Archivos desatendidos con la puerta abierta.
- Personas con ingreso al archivo, adicionales a las indicadas en el listado remitido por la SAF.
- Las llaves del Archivo 3 de la GCAU está al alcance de todo el personal.
- Cajas, bolsas y elementos diferentes a los que deben estar en un archivo de gestión.
- Ventana del archivo 1, de la Gerencia Tecnología, permanece abierta.
- El Archivo 2 de la Gerencia Comercial y Atención al usuario, tiene un rociador automático dentro del archivo, no se observó detector de humo dentro del archivo y una de las luminarias está caída.
- Se observó que en el archivo 4, Centro de Documentación, el personal de 4/72 hace uso de su celular en la zona de archivo.

S.E. Se realizó verificación de la información contenida en la "Carpeta temporal" o "tmp", la cual no tiene lineamientos establecidos para su uso, y se encontró información como por ejemplo: informes técnicos de avalúo catastral, certificaciones de información catastral, planos, archivos identificadores de predios, informes de plusvalía, entre otros, a los cuales se puede tener acceso sin ningún tipo de restricción, y que, como se comentó en el control A.9.3.1 Uso de información de autenticación secreta, también se puede acceder a través de los portátiles de la entidad, a los que se puede ingresar con el usuario y clave adheridos a ellos.

S.E. En los sitios de disposición del papel reciclaje y del reutilizable, se encontraron diferentes documentos: planos, correos electrónicos, comunicaciones sobre plusvalía, conceptos técnicos de avalúos, registros topográficos.

Hallazgo:

(OM) Con el fin de evitar el daño de la documentación conservada en el Archivo 2 de la GCAU, se debe revisar la posibilidad de anular el rociador automático que se encuentra dentro de él, así mismo, arreglar la luminaria. De igual manera, cerrar la ventana del archivo 1 de la Gerencia Tecnología.

(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció un incumplimiento a lo establecido en el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, código 02-02-PR-02, numeral 3.4.1. Restricciones de Acceso, Tabla 5, donde se indican las restricciones de acceso frente a la información pública clasificada o información pública reservada: "*a. Acceder a los activos de tipo dato/información previa autorización dada por el propietario del activo y asignación de un usuario y contraseña robusta (…). d. Acceder a los activos tipo dato/información a través del uso de mecanismos de doble factor de autenticación. (…)"*, por cuanto se observaron informes técnicos de avalúo catastral (información pública clasificada), certificaciones de información catastral (información pública clasificada), planos, archivos identificadores de predios, informes de plusvalía (información pública clasificada), entre otros, en la "Carpeta Temporal" que puede ser accedida sin ningún tipo de restricción por las personas que se autentiquen en la red de la Entidad, incluyendo la autenticación con los usuarios y claves adheridos en los equipos portátiles de la Unidad, lo que podría generar destrucción, falsificación, acceso no autorizado y liberación no autorizada de la información que captura, integra y dispone la UAECD.

(AC) A partir de la auditoría al SGSI de la UAECD 2019, se evidenció el incumplimiento a lo establecido en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, Política de Escritorio y Pantalla Limpios, numeral 2.3.4. Principios, "*o. Las impresiones que ya no sean requeridas y que contengan información clasificada o reservada no deben ser utilizadas como papel reciclable y deben ser trituradas antes de ser desechadas*" y en el numeral 2.7.3. Uso adecuado y consumo de papel, del Documento Técnico Reglamento de Uso de los Recursos Físicos y Funcionamiento de las Instalaciones de la UAECD, código 07-02-DT-01 y del Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, código 02-02-PR-02, numeral 3.4.1. Restricciones de Acceso, Tabla 5, donde se indica "*3) Las impresiones que ya no sean requeridas que posean información pública clasificada o información pública reservada, no deben ser utilizadas como papel reciclable y deben ser trituradas antes de ser desechadas*.", por cuanto se encontraron impresos: informes técnicos de avalúo catastral (pública clasificada), informes de plusvalía (pública clasificada), entre otros, en las bandejas destinadas al papel de reciclaje y reutilizable, lo que podría generar riesgos en el acceso a información sensible de la Unidad o documentación que esté protegida por normas sobre protección de datos personales.

A.18.1.4. Privacidad y protección de datos personales.

Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

S.E. Se observó que la entidad cuenta con la siguiente documentación: Política para el Tratamiento de Datos Personales, registrada en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, Documento Técnico de Medidas Administrativas, Técnicas y Legales para el Tratamiento de Datos Personales, código 02-02-DT-05, V.2 del 28/08/2019, los Procedimientos de Consulta y Reclamación de Datos Personales, código 02-02-PR-04, V.3 del 29/10/2019 y el de Acceso y Disposición de Información, código 05-01-PR-08, V.4 del 14/06/2019.

A.18.1.5 Reglamentación de controles criptográficos.

Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

S.E. La Oficial de Seguridad informó que este control no aplica aún, puesto que en Colombia no existen regulaciones sobre la utilización de controles criptográficos.

6.1.12.2. A.18.2 Revisiones de seguridad de la información. Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

A.18.2.1 Revisión independiente de la seguridad de la información.

Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

S.E. En el Acta No. 3 del 29 julio de 2019 del Comité Institucional de Control Interno, se aprobó la realización de la presente auditoría, la cual se ha desarrollado de acuerdo con lo programado.

A.18.2.2. Cumplimiento con las políticas y normas de seguridad.

Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

S.E. A través del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, código 02-02-DT-02, se establecen las responsabilidades de los jefes de dependencia (dirección, gerencias, subgerencias, oficinas) para cada una de las políticas del Subsistema de Gestión de Seguridad y Privacidad de la Información de la UAECD y durante la presente vigencia se ha evidenciado la revisión y modificación de los procedimientos que conforman al Sistema de Gestión Integral, de los diferentes procesos, con el acompañamiento de la Oficina Asesora de Planeación y Aseguramiento de Procesos.

A.18.2.3 Revisión del cumplimiento técnico.

Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

S.E. Se evidenció en el Plan de Trabajo del SGSI 2019, que se establecieron las siguientes actividades con el fin de verificar el cumplimiento técnico de los controles de seguridad:

1. *"Revisar la aplicación del Documento Técnico Controles de Seguridad de la Información para la construcción de software seguro"*. Programada para octubre de 2019, está pendiente de ejecución.
2. *"Revisar la aplicación de los instructivos de hardening implementados"*. Programada para diciembre de 2019.
3. *"Realizar un Informe de revisión sobre el uso y protección de datos de producción en ambientes de pruebas"*. Ejecutada en el mes de junio de 2019.
4. *"Realizar una revisión técnica de las aplicaciones después de cambios en la plataforma de operación sobre una muestra de las plataformas de operación (sistemas operativos, bases de datos) y sistemas de información"*. Ejecutada en el mes de noviembre de 2019.

6.2. Revisión riesgos y controles asociados al Subproceso Gestión de la Seguridad de la Información.

Se verificó que el Proceso Gestión Integral del Riesgo, tiene un riesgo asociado a seguridad de la información: "*Materialización, en más de una oportunidad, de incidentes de seguridad de la información cerrados mayor a la meta establecida*", cuyo riesgo residual es bajo y el cual no se ha materializado a la fecha de la presente auditoría.

6.3. Revisión riesgos y controles asociados al Subsistema de Gestión de la Seguridad y Privacidad de la Información - SGSI.

Se evidenció que la Unidad cuenta con documentación formal de los riesgos y controles que buscan asegurar los activos de información de la entidad, los cuales son registrados en el formato de Matriz de Riesgos de la Seguridad de la Información, código 02-02-FR-08, por los responsables de los procesos que se encargan de identificar, analizar, valorar y evaluar los riesgos y sus controles.

La UAECD cuenta con controles a los riesgos de activos de información, que permiten proveer un nivel de seguridad a la información que captura, integra y dispone, sin embargo, se observaron debilidades al momento de su implementación y aplicación.

De los diferentes procedimientos asociados al SGSI, se observó que el Procedimiento Control Ingreso y Salida de Personal a las Instalaciones y a las Áreas Seguras de la Unidad, código 07-03-PR-06, no tiene actividades de control; el Procedimiento Mantenimiento de aplicaciones, código 13-02-PR-19, tiene 7 actividades de control, sin embargo el procedimiento se encuentra en revisión para su modificación, por cuanto las actividades se están realizando de acuerdo al contexto interno actual de la Gerencia de Tecnología y no como estaban documentadas. Por último, el Procedimiento Traslado y Entrega de Elementos Devolutivos, código 07-01-PR-02, tiene controles que no están siendo efectivos o no se aplican, por cuanto el aplicativo SAI no se actualiza al momento de la devolución o traslado de equipos de cómputo, se lleva una relación en excel, como se observó en el informe de seguimiento derechos de autor software, lo cual ha causado posibles diferencias en los inventarios y la no localización de equipos de cómputo.

6.4. Oficial de Seguridad de la UAECD.

6.4.1. Resolución interna 890 de 2018, numeral 3.3. Oficial de Seguridad.

En cuanto a la persona designada como Oficial de Seguridad, se procedió a la verificación de las acciones específicas designadas a través de la Resolución Interna 890 de 2018, "*Por la cual se adopta el Modelo Integrado de Planeación y Gestión y se crea el Comité Institucional de Gestión y Desempeño de la Unidad Administrativa Especial de Catastro Distrital*", numeral 3.3. Oficial de Seguridad.

A través de las diferentes entrevistas y de las evidencias aportadas por la Oficial de Seguridad durante la ejecución de la presente auditoría, se pudo establecer que ha dado cumplimiento a las responsabilidades asignadas en la Resolución Interna 890 de 2018, en cuanto a que se han proyectado, propuesto, presentado para aprobación las políticas, normas, acciones o buenas prácticas necesarias para incorporar y/o aplicar en la gestión de la seguridad de la información en la entidad. De igual forma, la Profesional designada ha identificado los procesos críticos de la operación y los sistemas de información asociados que provee la UAECD y, propende permanente por el cumplimiento de los lineamientos que se han implementado. Finalmente, lidera las campañas de socialización a los servidores públicos con el fin de lograr la apropiación y aplicación del Subsistema de Gestión de Seguridad y Privacidad de la Información.

6.4.2. Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2). Versión 7, abril de 2019.

De acuerdo con lo establecido en el Manual de Gobierno Digital, versión 7, abril de 2019, en su numeral 1.6. Responsables de la Política, se indica que "***Responsable de Seguridad de la Información****: (…) se debe designar un Responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección (MIPG, 2017). (…)".*

El Responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo designado en cada entidad y tendrá las responsabilidades establecidas en la guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (Guía 4 - Roles y Responsabilidades), quien, a su vez, tiene responsabilidades asignadas dentro de cada dominio del Marco de Arquitectura Empresarial. El responsable de seguridad de la información deberá participar en los comités de desempeño institucional.

Así mismo, el responsable de seguridad de la información debe apoyar a los líderes de los procesos o áreas de la entidad, con el objetivo de implementar adecuadamente los lineamientos, esto incluye la identificación de los activos y los riesgos derivados en estos.

De igual manera, el responsable de seguridad de la información se debe apoyar fundamentalmente en el CIO[4] de la entidad para mitigar los riesgos asociados a la tecnología (Seguridad Informática o Ciberseguridad), también se debe apoyar en otras áreas que permitan mitigar otros tipos de riesgos de seguridad de la información, Ej. Recursos Físicos, Talento Humano entre otras

(…) NOTA: Para lograr un adecuado balance entre funcionalidad y seguridad, se recomienda que el elemento transversal de seguridad de la información opere de manera independiente a la Oficina de T.I. En este caso, la entidad puede ubicar esta iniciativa en un área como planeación, procesos, el área relacionada con gestión de riesgos, o bien, crear una nueva área dedicada a la seguridad de la información. (…)

Se evidenció que la Oficial de Seguridad participó en los Comités Institucionales del 12/06/2019 y del 14/08/2019, según consta en las Actas 20 y 23 respectivamente, presentando temas relacionados con el Subsistema de Seguridad y Privacidad de la Información - SGSI. Así mismo, en los Comités del 03/07/2019 y del 13/09/2019, el encargado de presentar los temas relacionados con el SGSI fue el Gerente de Tecnología, no se contó con la presencia de la Oficial de Seguridad.

Recomendación: Evaluar una mayor participación del responsable de seguridad de la información en los comités de desempeño institucional, tal y como se menciona en el Manual de Gobierno Digital; así mismo, considerar que el cargo de Oficial de Seguridad pertenezca a un área que haga parte del direccionamiento estratégico o Alta Dirección, y que opere de manera independiente a la Oficina de T.I., con el fin de evitar posibles conflictos de intereses y funciones.

7. FORTALEZAS

Se evidenció que, de los 114 controles establecidos en la norma, la Entidad tiene documentados 111 de ellos, 2 están en proceso de revisión y aprobación, y 1 de ellos no aplica actualmente (A.18.1.5), lo que evidencia el avance de la Unidad en la documentación y establecimiento de controles en pro del mejoramiento de la seguridad y privacidad de la información que se captura, integra y dispone.

Se resalta el esfuerzo por parte de los responsables de procesos y la Oficial de Seguridad, en cuanto a la actualización de los documentos técnicos, procedimientos, instructivos, entre otros, que hacen parte del Subsistema de Gestión de Seguridad de la Información -SGSI.

Se evidenció la disposición y colaboración por parte de los servidores públicos, en especial al Equipo de Seguridad de la Información, durante el desarrollo de la Auditoría, así como la atención, importancia y respeto que se dio durante el desarrollo de esta.

8. CONCLUSIONES

De acuerdo con el objetivo general y los específicos, planteados al inicio del ejercicio auditor, se concluye que el uso y apropiación de los lineamientos definidos para el SGSI en la UAECD presenta un nivel adecuado, teniendo en cuenta que las socializaciones sobre el Subsistema

[4] **CIO** (Chief Information Officer) o director de tecnología.

iniciaron en la presente vigencia, sin embargo, a lo largo del presente informe se dan recomendaciones para los puntos que son susceptibles de mejora.

En cuanto a determinar la conformidad del Subsistema de Seguridad y Privacidad de la Información de la UAECD con los requisitos establecidos en la norma ISO 27001:2013, tomando como base la información de la Declaración de Aplicabilidad del 26/02/2018 y la que se evidenció durante la presente auditoría, se observa el avance que ha tenido la UAECD en cuanto a la documentación que exige la norma ISO 27001:2013 y, los controles de Seguridad y Privacidad de la Información en el marco del Modelo de Seguridad y Privacidad de TI de MinTIC, así: en el 2018 la entidad tenía documentados e implementados o en proceso de implementación 70 de 113 controles que le aplican a la Unidad, equivalente al 62%, actualmente se tienen documentados y oficializados 41 controles más (36%), lo que da un total del 111 controles documentados (98% de los 113 controles, del total de 114 de la norma ISO 27001:2013, el control A.18.1.5 no aplica). Por otra parte, la Unidad debe avanzar en el monitoreo periódico de los activos de información de la Entidad, evaluar la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia y, utilizar indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información, con el fin de avanzar en el nivel de madurez de la implementación.

La entidad se encuentra en proceso de implementación del Subsistema de Seguridad y Privacidad de la Información, se evidencia la existencia de elementos y controles que permiten proveer una protección a la información de la Unidad, sin embargo, no se evidenció un indicador que mida el nivel de madurez en la implementación de controles de seguridad.

De acuerdo con lo evidenciado durante la presente auditoría y a las características de los niveles de madurez establecidos por Mintic en su Modelo de Seguridad y Privacidad de la Información (son 6 niveles que inician desde el nivel 0), la UAECD se encuentra en el nivel 3, "***Definido***: • *La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.* • *La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.* • *La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.* • *La Entidad tiene procedimientos formales de seguridad de la Información* • *La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.* • *La Entidad ha realizado un inventario de activos de información aplicando una metodología.* • *La Entidad trata riesgos de seguridad de la información a través de una metodología.* • *Se implementa el plan de tratamiento de riesgos.* • *La entidad cuenta con un plan de transición de IPv4 a IPv6.".*

Por último, se aclara que los resultados de este informe se refieren sólo a las evidencias obtenidas de acuerdo con los criterios definidos, documentos aportados y a la información verificada y no se hacen extensibles a otros soportes u acciones realizadas con posterioridad a la auditoría

9. RECOMENDACIONES

Como resultado de la presente auditoría se encontraron 8 oportunidades de mejora y 7 acciones correctivas. Igualmente, se plantearon 59 recomendaciones, 46 de ellas incluyen la actualización de la Declaración de Aplicabilidad.

En el Anexo No. 1, CONSOLIDADO DE LA REVISIÓN EFECTUADA POR LA OCI, A LA IMPLEMENTACIÓN DE LOS DOMINIOS (14), OBJETIVOS (35) Y CONTROLES DE SEGURIDAD (114) INDICADOS EN LA NORMA ISO 27001:2013, se indican los 46 ítems de la Declaración de Aplicabilidad que se deben actualizar en el mes de diciembre de 2019, de acuerdo con lo programado en el Plan de Acción Institucional de la presente vigencia y lo evidenciado en la presente auditoría.

Adicionalmente, se recomienda construir un indicador que mida el nivel de madurez en la implementación de controles de seguridad en la Unidad, con el fin de tomar las medidas requeridas para alcanzar los niveles superiores (Administrado y Optimizado), que sugiere MinTic en su Modelo de Seguridad y Privacidad de la Información.

Las recomendaciones fueron planteadas a lo largo del informe, para los controles de la Declaración de Aplicabilidad de la Unidad que lo hayan ameritado, y es potestad de la Administración acogerlas y establecer un plan de acción para ellas.

Finalmente, se informa que se procederá a realizar el registro de las acciones correctivas en el ISODOC para que procedan a realizar el análisis de causas e implementación de acciones acorde con lo indicado en el Procedimiento Acciones de Mejora, código 14-01-PR-02.

ORIGINAL FIRMADO

JOHNY GENDER NAVAS FLORES
Jefe Oficina de Control Interno

Con copia: Ligia Elvira González Martínez – Gerencia Comercial y de Atención al Usuario
José Luis Ariza – Gerencia de Tecnología
Pamela del Pilar Mayorga – Gerencia IDECA
Manuel Duglas Raúl Ávila – Oficina Asesora Jurídica
Rosalbira Forigua – Subgerencia de Recursos Humanos
Victor Alonso Torres – Subgerencia Administrativa y Financiera

Anexo No. 1, Consolidado de la Revisión Efectuada por la OCI, a la Implementación de los Dominios (14), Objetivos (35) y Controles de Seguridad (114) indicados en la Norma ISO 27001:2013

Elaboró y Verificó: Astrid Yasmin Villanueva C. - Contratista Oficina de Control Interno
Revisó: Johny Gender Navas Flores