



UAECD
Catastro Bogotá

UNIDAD ADMIN. CATASTRO DISTRITAL 14-08-2020 04:27:53

Al Contestar Cite Este Nr.:2020IE9173 O 1 Fol:1 Anex:0

ORIGEN: Sd:77 - OFICINA DE CONTROL INTERNO/NAVAS FLORES JO

DESTINO: DIRECCION GENERAL/RODRIGUEZ SOSA HENRY/ DIRECTO

ASUNTO: INFORME FINAL AUDITORIA SGSI 2020

OBS: PROYECTO / YASMIN VILLANUEVA

MEMORANDO

Referencia: Plan Anual de Auditorías de la UAECD vigencia 2020.

FECHA: 14 de agosto de 2020

PARA: Henry Rodríguez Sosa
Director Unidad Administrativa Especial de Catastro Distrital

DE: Johnny Gender Navas Flores
Jefe Oficina Control Interno

ASUNTO: Informe final de la Auditoría de Gestión de Seguridad y Privacidad de la Información.

En cumplimiento del Plan Anual de Auditorías de la UAECD vigencia 2020, la Oficina de Control Interno en el marco de sus actividades orientadas al fortalecimiento del Sistema de Control Interno de la Unidad, realizó el informe de la “Auditoría de Gestión de Seguridad y Privacidad de la Información”, como parte del proceso misional de la Unidad, el cual se remite para su conocimiento y demás fines pertinentes.

A continuación, relacionamos las principales fortalezas, conclusiones y recomendaciones:

FORTALEZAS

El Subsistema de Gestión de Seguridad y Privacidad de la Información se encuentra alineado con los objetivos de la UAECD, lo cual convierte a la seguridad en un habilitador de negocio y en un elemento para lograr que los riesgos no se materialicen ni perjudiquen el desarrollo de las actividades que adelanta la entidad tanto internas como externas.

La participación de las áreas y su personal (funcionarios y contratistas) en la aplicación de controles, así como en las sensibilizaciones y capacitaciones realizadas, hacen que el sistema avance en apropiación y por lo tanto su sostenibilidad a mediano plazo pueda ser mantenida. Igualmente, se observaron estrategias, actividades, acciones permanentes que buscan el constante mejoramiento del Subsistema.

CONCLUSIONES

Teniendo en cuenta los objetivos de la presente auditoría, en cuanto a verificar el uso y apropiación de los lineamientos definidos para el SGSI en la UAECD y con el alcance de verificar y evaluar el cumplimiento de lo establecido en los controles A.5. a A.9. del Anexo Técnico de la norma ISO 27001:2013, se puede concluir que la entidad tiene documentados e implementados los 39

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90

Código postal: 111311

Torre A Pisos 11 y 12 – Torre B Piso 2

Tel: 2347600 – info: Línea 195

www.catastrobogota.gov.co

Trámites en línea: catastroenlinea.catastrobogota.gov.co



MEMORANDO

controles establecidos en la norma, los cuales son susceptibles de mejora teniendo en cuenta los hallazgos registrados a lo largo del presente informe, para los cuales se deberá establecer un plan de mejora.

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

RECOMENDACIONES

Como resultado de la presente auditoría se encontraron 4 oportunidades de mejora y 2 acciones correctivas. Igualmente, se plantearon 7 recomendaciones a lo largo del informe.

Adicionalmente, se sugiere 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 las siguientes:

- Teniendo en cuenta el plazo establecido para la implementación de las políticas, adicional a los resultados de la presente auditoría, la entidad debe tener mecanismos para evaluar el porcentaje de avance de apropiación de las 12 políticas detalladas de seguridad y privacidad de la información, con el fin de realizar los ajustes, de ser necesario, para dar cumplimiento a la fecha establecida.
- Dado que en la auditoría realizada por la Oficina de Control Interno durante la vigencia 2019, no se evidenció en las actas del Comité Institucional de Gestión y Desempeño 2019 la revisión de las políticas de seguridad de la información, se sugiere que una vez surtido el proceso de revisión de las políticas detalladas, el documento final sea remitido al comité institucional para su revisión y aprobación, dejando constancia en la respectiva acta, para dar cumplimiento a la función asignada en la Resolución 890 de 2018. Igualmente, una vez aprobado el documento antes mencionado y la resolución por la cual se adoptará la Política de Seguridad y Privacidad de la Información de la Unidad, se sugiere socializarlos a través de las capacitaciones que se realizan a todo el personal sobre el SGSI.
- Reforzar a través de las capacitaciones en línea y/o presenciales, y a través del envío de tips de información por correo electrónico, las responsabilidades que cada uno de los actores de la Unidad tiene en el SGSI, así como de las sanciones a que haya lugar por su incumplimiento.
- Se sugiere revisar la conveniencia de impedir el procesamiento y el almacenamiento de información pública reservada e información pública clasificada sobre el equipo de propiedad privada, con el fin de mitigar los riesgos en los activos de información.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso 2
Tel: 2347600 – info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co



MEMORANDO

- Con el fin de evitar la materialización de los riesgos “Trámite de los procesos de selección y vinculación de manera inoportuna y/o sin el cumplimiento de los requisitos legales.” y “Posible omisión del análisis de la documentación presentada por el candidato que se va a vincular, quien incluso puede presentar certificaciones falsas sin que éstas sean detectadas, en beneficio particular.”, se sugiere estudiar la posibilidad de realizar un análisis de los diferentes cargos de la Unidad y establecer una clasificación de acuerdo con su nivel de responsabilidad y rol en la entidad, a la clasificación de la información a la que podrán acceder de acuerdo con el registro de activos de información, tanto digital como física (nivel de acceso y los permisos que tendrán sobre la información), con el propósito de determinar qué cargos deben someterse a una revisión de antecedentes, estudios, experiencia laboral y profesional más riguroso, y evitar la materialización de riesgos de corrupción y proceso relacionados con el manejo de información de la Unidad.
- Se sugiere implementar una estrategia de cierre de brecha, aplicando una encuesta de conocimiento antes y después de cada capacitación o socialización, con el fin de determinar la efectividad de estas.
- Recomendación: A partir de la auditoría al SGSI de la UAECD 2020, se evidenciaron correos de personal retirado desde hace 4 meses o más, que aún aparecen en el directorio de correos de la Unidad, a pesar de sus usuarios fueron desactivados como lo indica el Procedimiento Gestión de Accesos, código 13-02-PR-04, numeral 3.1.1. Novedades de personal y contractuales. Por lo anterior, se sugiere revisar las causas de esta desviación y que no aparezcan como activos o que al momento de enviar un mensaje a estos correos sea devuelto un mensaje indicando que la persona ya no se encuentra vinculada con la Unidad.

Cordialmente,



JOHNY GENDER NAVAS FLORES
Jefe Oficina Control Interno

Con copia: María Clara Rodríguez – Jefe OAPAP
Helvert Alberto Guzmán – Jefe Oficina Asesora Jurídica
Mayiver Méndez Sáenz – Jefe Oficina Control Disciplinario
Hector Henry Pedraza – Gerente de Tecnología
Luis Javier Clevez – Gerente de Gestión Corporativa
Rosalbira Forigua – Subgerente de Recursos Humanos

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

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso 2
Tel: 2347600 – info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co



 <p>UAECD Catastro Bogotá</p>	<h2>INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO</h2>
---	--

Seleccionar tipo de Informe:

Evaluación Seguimiento Auditoría de Gestión

En cumplimiento del Plan Anual de Auditorías de la vigencia **2020**, a continuación, se presentan los resultados del Informe citado dirigido al director 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 en los controles A.5. a A.9. del Anexo Técnico de la norma ISO 27001:2013, 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 UAECD, de enero 01 a junio 30 de 2020.

4. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA

- La norma ISO 27001 versión 2013.
- Subproceso Gestión de Seguridad de la Información, código 02-SP-02.
- Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, Código: 02-02-DT-02, 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 3, 2020.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

- Procedimiento Gestión de Accesos, código: 13-02-PR-04, versión: 6 del 10/09/2019.
- Procedimiento Gestión de Incidentes de Seguridad de la Información, código 02-02-PR-01, versión 6, fecha 30/04/2020.
- Procedimiento Gestión de Activos en el marco de la seguridad de la información, código 02-02-PR-02.
- Subproceso Selección, Vinculación y Retiro de Personal, código 06-SP-01 v.5.
- Procedimiento Teletrabajo, código 06-05-PR-03.
- Procedimiento Gestionar Retiro de Personal, código 06-01-PR-02
- Documentos Técnicos, Instructivos, Formatos y demás documentos relacionados con el objetivo de la auditoría.
- Modelo de Seguridad de la Información - MinTic, versión 1 del 08/04/2016.
- Guía No. 8 del Mintic “Controles de Seguridad y Privacidad de la Información”.
- Demás normatividad interna y externa relacionada con el objetivo 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.

La Oficina de Control Interno convocó nuevamente a los auditores internos en la norma ISO 27001:2013 que participaron en la auditoría de la vigencia 2019, conformando el equipo auditor así: Astrid Yasmin Villanueva, contratista de la OCI y auditor líder, auditoras internas: Angela Indira Suarez, Diana Hasbleidy Calderón y Sandra Lucía Rincón.

Para el desarrollo de la auditoría se tuvieron en cuenta las condiciones dadas por la cuarentena por covid-19 y las herramientas que la Unidad ha dispuesto para el desarrollo de las diferentes labores.

Así, 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 y, la “Declaración de Aplicabilidad 2020”¹.

Basados en los documentos antes mencionados, se procedió a la revisión de la información remitida por las diferentes áreas requeridas y la documentación publicada en el ISODOC, y se aplicó una encuesta a los usuarios de las áreas de Dirección, Gerencia de Información Catastral, Oficina de Comunicaciones y la Subgerencia de Información Económica, con el fin de verificar el uso y apropiación de los lineamientos de las políticas detalladas y los procedimientos relacionados con los controles a evaluar de la ISO 27001:2013 (Controles A.5 a A.9).

¹ Documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad).

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





Así mismo, se realizaron entrevistas virtuales con la Oficial de Seguridad, personal de soporte del aplicativo Cordis, la Profesional de la Subgerencia de Recursos Humanos designada para atender la auditoría, entre otros.

6. PRESENTACIÓN DE RESULTADOS

6.1. Revisión Declaración de Aplicabilidad.

Para la presentación de resultados se tomó como base la Declaración de Aplicabilidad de la UAECD, V.3., del 10/12/2019 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. Para la presente auditoría se tomaron los controles del A.5. al A.9.

A continuación, se muestra el consolidado de la revisión efectuada por la OCI, a la implementación de los 5 dominios, 13 objetivos y 39 controles de seguridad indicados en la norma ISO 27001:2013 para los controles A.5 al A.9, y el control descrito en la Guía No. 8 del Mintic “Controles de Seguridad y Privacidad de la Información”.

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.

- 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 29/10/2019, 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.
- El plazo para la implementación de estas políticas es diciembre de 2020.

Recomendación: Teniendo en cuenta el plazo establecido para la implementación de las políticas, adicional a los resultados de la presente auditoría, la entidad debe tener mecanismos para evaluar el porcentaje de avance de apropiación de las 12 políticas detalladas de seguridad y privacidad de la información, con el fin de realizar los ajustes, de ser necesario, para dar cumplimiento a la fecha establecida.

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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

- 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 continuas*
- Se encontró que una de las funciones asignadas al Comité Institucional de Gestión y Desempeño, a través de la Resolución interna 890 de 2018, es “*h. Funciones relacionadas con la Gestión de Seguridad de la Información*”, numerales “*1. Aprobar las estrategias y políticas de seguridad de la información que requiera la Unidad de acuerdo con la dinámica y condiciones de operación*” y “*3. Evaluar y aprobar las políticas básicas y específicas de seguridad de la información, garantizando su difusión y aplicación en la Entidad.*”.
- El documento de políticas detalladas fue modificado en 2 ocasiones durante la vigencia 2019.
- Al momento de la auditoría, el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, Código: 02-02-DT-02, versión 6 del 29/10/2019, se encuentra en revisión por parte de la Ofical de Seguridad de la Información y la contratista que apoya a la Oficial en el desarrollo de los temas del SGSI, una vez se surta esta revisión, se procederá a realizar mesas de trabajo para validar con otras áreas las responsabilidades en las políticas.
- Por último, se evidenció, como parte de la evidencia de la OPOR-2019-0034, registrada en el ISODOC, el proyecto de resolución “*Por la cual se adopta la Política de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Catastro Distrital*”, que se encuentra en revisión para ser aprobada por parte del Comité Institucional de Gestión y Desempeño, y que incluye el “*Artículo 6: Revisión De La Política: La UAECD revisará la Política de Seguridad y Privacidad de la Información y las políticas detalladas derivadas con una periodicidad mínima anual o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.*”

Recomendación

Teniendo en cuenta que, en la auditoría realizada por la Oficina de Control Interno durante la vigencia 2019, no se evidenció en las actas del Comité Institucional de Gestión y Desempeño 2019 la revisión de las políticas de seguridad de la información, se sugiere que una vez surtido el proceso de revisión de las políticas detalladas, el documento final sea remitido al comité institucional para su revisión y aprobación, dejando constancia en la respectiva acta, para dar cumplimiento a la función asignada en la Resolución 890 de 2018. Igualmente, una vez aprobado el documento antes mencionado y la resolución por la cual se adoptará la Política de Seguridad y Privacidad de la Información de la Unidad, se sugiere socializarlos a través de las capacitaciones que se realizan a todo el personal sobre el SGSI.

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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





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

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.

- 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, 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.
- Mediante correo electrónico de 09 de julio de 2020, la Oficial de Seguridad indica que: "*Todos los funcionarios y contratistas firman 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", la Oficina Asesora Jurídica y la Subgerencia de Recursos Humanos verifican el cumplimiento a la firma del compromiso en contratistas y funcionarios.*", información que fue verificada con las respectivas áreas.
- En la Política de Control de Acceso definida en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, versión 6 de 29/10/2019, se encuentran definidas las responsabilidades asociadas al cumplimiento de los objetivos y principios para cada una de ellas.
- Con el fin de validar el conocimiento y apropiación del SGSI, se realizó encuesta a través de la herramienta Microsoft forms, la cual fue aplicada del 13 al 15 de julio a 4 áreas de la entidad y contestada por 102 de sus funcionarios y contratistas, distribuidos así:

1. Área en la que desarrolla sus actividades:

[Más detalles](#)

● Dirección	5
● Oficina Asesora de Comunicac...	2
● Gerencia de Información Cata...	51
● Subgerencia de Información E...	44



2. Tipo de vinculación

[Más detalles](#)

● Funcionario (carrera administr...	67
● Contratista	35



A la pregunta “¿Considera ud. que hace parte activa del Subsistema de Seguridad y Privacidad de la Información?”, 100 de las 102 personas respondieron de forma positiva y reconocen (mencionaron en la encuesta) una o más responsabilidades frente al SGSI. Así mismo, a la afirmación “Los contratistas no tienen sanciones por faltas a la seguridad de la información.”, 98 de las 102 personas reconocieron que los contratistas si están expuestos a faltas por no dar cumplimiento a los lineamientos establecidos de seguridad y

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





privacidad de la información, por último, a la afirmación “*La Política de uso aceptable no aplica para personal externo.*” 76 de los 102 encuestados respondieron de manera correcta (falso). Lo anterior muestra, que un alto porcentaje del personal (planta y contratistas) de la Unidad reconoce que tiene responsabilidades frente al SGSI y aunque no hay total claridad de las responsabilidades detalladas, si en la generalidad de estas, así mismo identifica que el personal externo también está en la obligación de cumplir con los lineamientos del Subsistema.

Recomendación:

Reforzar a través de las capacitaciones en línea y/o presenciales, y a través del envío de tips de información por correo electrónico, las responsabilidades que cada uno de los actores de la Unidad tiene en el SGSI, así como de las sanciones a que haya lugar por su incumplimiento.

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.

- Se evidencia la separación de deberes en la definición de la Política de Control de Acceso ítem 2.2 del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, v.6 de 29/10/2019, a través de la asignación de cuentas de usuario donde, para cada cuenta, tiene asignado un rol dependiendo de las labores a realizar.
- Se evidencia en el Procedimiento Mantenimiento de Aplicaciones, código 13-02-PR-19, v.4 de 12/05/2020 se encuentra definidos los ambientes para el desarrollo de las actividades del procedimiento (Ambiente de Desarrollo, Ambiente de Pruebas y Ambiente de Producción), al igual que los roles o equipos operativos definidos para la gestión del procedimiento (Equipo de análisis, diseño y construcción, Equipo de pruebas, Equipo gestión paso producción, verificación y cierre).
- Igualmente, se observa la separación de deberes en otros procesos y procedimientos como los que componen la Gestión Presupuestal, la Gestión de Tesorería, la Gestión Contable, entre otros, como lo ha podido verificar la Oficina de Control Interno a través de sus auditorías, seguimientos y evaluaciones.

A.6.1.3 Contacto con las autoridades.

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

- Mediante correo electrónico de 09 de julio de 2020, la Oficial de Seguridad adjuntó archivo en Excel “Contacto de Autoridades 2020”, que contiene información de autoridades internas, externas distritales, de seguridad y de emergencia.

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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





- Mediante correo electrónico de 09 de julio de 2020, la Oficial de Seguridad adjuntó el archivo en Excel, “Grupo de Interés 2020” que contiene los grupos de interés en seguridad de la información a nivel nacional e internacional.

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.

- La Unidad tiene establecido el Procedimiento Mantenimiento de aplicaciones, código 13-02-PR-19, v.4 del 12/05/2020, para la gestión de proyectos de software desarrollados por la entidad.
- 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.

- 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. No obstante, no existe un instructivo, procedimiento u otro lineamiento que permita verificar el cumplimiento de la política en todo momento, tales como la asignación de privilegios, borrado seguro de la información y aplicación de técnicas de cifrado.
- En entrevista con funcionario de la Subgerencia Administrativa y Financiera, cargo Técnico operativo, encargado de los equipos móviles, se evidenció que:
 - Existe un inventario de dispositivos móviles actualizado.
 - No hay claridad respecto a la responsabilidad de la mesa de servicios de TI en cuanto a la configuración estándar de los dispositivos móviles propiedad de la entidad.
 - No existe un formato que permita verificar el borrado de la información y/o formateo del dispositivo móvil a configuración de fábrica.
 - Por seguridad se le solicita a la persona que devuelva el dispositivo móvil a almacén, el elemento debe estar restaurado de fábrica o de lo contrario se pide una autorización verbal a la persona que utilizaba el dispositivo para realizar dicha acción por parte del almacén.
- En entrevista con la encargada de la mesa de servicios, mencionó que el lineamiento para dispositivos móviles es el que está establecido en la política y que una vez se coloca la mesa de servicios, se llevan a

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

cabo unos pasos para su configuración, sin embargo, los únicos parámetros establecidos están en la política para dispositivos móviles.

(AC) A partir de la Auditoría al SGSI 2020, se evidenció que no se tiene un estándar para la configuración de los dispositivos móviles de propiedad de la Unidad, ni un instructivo o procedimiento para realizar las actividades a que haya lugar para configuración y borrado de los equipos en mención, incumpliendo con lo establecido en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, 2.9.5. Responsabilidades, “iii. Mesa de servicios de TI: i. Definir y aplicar un estándar de configuración para los dispositivos móviles propiedad de la Unidad. ii. Realizar las actividades de instalación de software autorizado por la Unidad y desinstalación de software en los dispositivos móviles.”, lo que podría generar la materialización de riesgos de seguridad de la información que conlleva el acceso a la información de la Unidad por medio de dispositivos móviles como pérdida o robo de información y de los dispositivos móviles, Uso de sistemas de conexión no seguros, entre otros.

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.

- 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. Como producto de una acción correctiva de la auditoría al SGSI vigencia 2019, la Subgerencia de Recursos Humanos y la Oficial de Seguridad, trabajaron en la elaboración de la política de teletrabajo, de la cual se observó el borrador de la resolución, que será remitido en el mes de julio de 2020 para revisión por parte de la abogada de SRH, la Subgerente de Recursos Humanos y el Gerente Corporativo.
- Procedimiento Teletrabajo, asociado al proceso Gestión del Talento Humano. Código 06-05-PR-03, v. 3, del 10/05/2019.
- En entrevista con la Oficial de la Seguridad indica que se está trabajando en los temas de seguridad de la información para el trabajo en casa, ya que se tenía contemplado solamente el teletrabajo.
- Por otra parte, de las 102 personas que contestaron la encuesta, 30 manifestaron no tener conocimiento o haber recibido lineamientos de seguridad de la información para realizar trabajo remoto o trabajo en casa, no obstante, el equipo auditor observó indicaciones de seguridad remitidas a través de comunicaciones internas.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





17. ¿Ha recibido lineamientos de seguridad de la información por parte la UAECD para realizar el trabajo remoto actual?

[Más detalles](#)

SI 72
NO 30



(OM) A partir de la Auditoría al SGSI 2020, se evidenció que, aunque se han dado lineamientos de seguridad de la información para el trabajo en casa adelantando con motivo del covid-19, no se observa la suficiente apropiación o reconocimiento de la información por parte del personal de la Unidad, lo que podría generar la mala utilización de herramientas de la Unidad y de los activos de información.

Recomendación:

Se sugiere revisar la conveniencia de impedir el procesamiento y el almacenamiento de información pública reservada e información pública clasificada sobre el equipo de propiedad privada, con el fin de mitigar los riesgos en los activos de información.

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.

- 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. 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 carpeta 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.
- Se observaron los siguientes documentos en el Sistema Integrado de Gestión, los cuales tienen actividades de verificación de requisitos mínimos de las personas que se vincularán como funcionarios de la entidad:

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

- Procedimiento de Selección y Vinculación de Provisionales, código 06-01-PR-03, V.4, 21/10/2019, actividad de control 6. *Verificar requisitos mínimos de aspirantes y 18. Diligenciar formato de análisis de requisitos mínimos.*
- Procedimiento de Selección y Vinculación de Servidores de Libre Nombramiento y Remoción, código 06-01-PR-04, v.1, 08/11/2017, actividad de control 18. *Verificar documentación.* A pesar de ser una actividad de control, la misma no indica específicamente cómo se debe realizar la verificación.
- Procedimiento Selección y Vinculación Período de Prueba (aplica para elegibles carrera administrativa), código 06-01-PR-06, V.3, 29/10/2018, actividades de control: 18. *Recibir y verificar requisitos del elegible.* (Profesional de Selección, 30. *Confirmar cumplimiento de requisitos mínimos* (Profesional de Vinculación).

Para el personal que ocupará cargos en planta (provisionalidad, libre nombramiento, periodo de prueba en el caso de carrera administrativa) si bien los procedimientos de selección tienen establecidas actividades de control para la verificación de requisitos mínimos sobre la hoja de vida aportada por los aspirantes y sus soportes, la misma no es una actividad para la confrontación juiciosa de la veracidad de los documentos aportados por los aspirantes (estudios, experiencia laboral y profesional relacionada), por lo cual una de las oportunidades de mejora resultado de la Auditoría a la 1ª Dimensión del MIPG - Talento Humano en cuanto a la verificación de estudios, se registró como la OPOR-2020-0061: “A partir de la Auditoría a la 1ª Dimensión del MIPG – Talento Humano vigencia 2020, se observó que el Procedimiento Selección y Vinculación de Provisionales, código 06-01-PR-03, no tiene establecido una actividad/control que indique concretamente la verificación de los estudios de pregrado y postgrado del personal que ingresa en calidad de provisionalidad, y que se toman como base para la liquidación de la prima técnica, lo que podría conllevar a que el personal no cumpla con todos los requisitos exigidos para ejercer el cargo para el cual es seleccionado y que la entidad pague prima técnica sin el lleno de requisitos legales”, que se encuentra en curso hasta el 30/09/2020.

Es de aclarar que siguiendo los lineamientos de la Circular Conjunta 052 de 2020 de la Secretaría General, la Secretaría Jurídica Distrital y el Departamento Administrativo del Servicio Civil, la Unidad tiene dos meses a partir del 06 de julio de 2020, para verificar títulos de idoneidad profesional (incluida la tarjeta profesional de ser el caso) así como lo concerniente a la experiencia laboral y profesional relacionada del personal de libre nombramiento y remoción.

Así las cosas, no se evidencia un control para verificar el perfil del candidato en relación con su confiabilidad (estudios, experiencia laboral y profesional), si va a desempeñar una tarea sensible para la organización en materia de Seguridad de la Información, se realiza verificación documental basada en el principio de la buena fe y prueba de conocimientos técnicos (dependiendo de las labores que desempeñará) durante el período de selección.

- Igualmente, para contratistas persona natural, se observó que el Procedimiento Contratación Directa, código 11-01-PR-05, v.3. 03/09/2018, que incluye la actividad de control 12. *Revisar la Solicitud*, “(...) *Verificar el perfil del contratista con los soportes presentados. (...) Verificar dentro de las páginas de los órganos de control los certificados respectivos, para lo cual se dejará anotación en los soportes. (...)*”, no

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

obstante, la revisión es solamente documental en cuanto a la verificación de la experiencia laboral y profesional relacionada.

También se revisó el Procedimiento Elaboración de Estudios Previos y Documentos Previos, asociado al Proceso Gestión Contractual, v.2., código 11-01-PR-02 del 20/10/2017 y los formatos Anexo Estudios Previos Prestación de Servicios Profesionales y de Apoyo a la Gestión – Análisis de Sector, código 11-01-FR-10 y Matriz de Asignación de Riesgos Previsibles, código 11-01-FR-13, los cuales no contemplan específicamente, ni indican que se deban contemplar, los riesgos de seguridad y privacidad de la información. Igualmente, en el formato Verificación Hoja de Vida, 11-01-FR-15, v. 1,3. no se evidencia un control para la verificación de autenticidad de los soportes aportados por el futuro contratista.

Recomendación: *De acuerdo con el correo remitido por la Subgerencia de Recursos Humanos del 11 de agosto de 2020, con la debida sustentación, se pasa la oportunidad de mejora a una recomendación,*

Con el fin de evitar la materialización de los riesgos “*Trámite de los procesos de selección y vinculación de manera inoportuna y/o sin el cumplimiento de los requisitos legales.*” y “*Posible omisión del análisis de la documentación presentada por el candidato que se va a vincular, quien incluso puede presentar certificaciones falsas sin que éstas sean detectadas, en beneficio particular.*”, se sugiere estudiar la posibilidad de realizar un análisis de los diferentes cargos de la Unidad y establecer una clasificación de acuerdo con su nivel de responsabilidad y rol en la entidad, a la clasificación de la información a la que podrán acceder de acuerdo con el registro de activos de información, tanto digital como física (nivel de acceso y los permisos que tendrán sobre la información), con el propósito de determinar qué cargos deben someterse a una revisión de antecedentes, estudios, experiencia laboral y profesional más riguroso, y evitar la materialización de riesgos de corrupción y proceso relacionados con el manejo de información de la Unidad.

(OM) A partir de la Auditoría al SGSI 2020, teniendo en cuenta la Circular Conjunta 052 de 2020 y para evitar la materialización del riesgo “*Posible omisión del análisis de la documentación presentada por el candidato que se va a vincular, quien incluso puede presentar certificaciones falsas sin que éstas sean detectadas, en beneficio particular.*”, se recomienda modificar en el Procedimiento de Selección y Vinculación de Servidores de Libre Nombramiento y Remoción, código 06-01-PR-04 la actividad de control para verificar títulos de idoneidad profesional (incluida la tarjeta profesional de ser el caso) así como lo concerniente a la experiencia laboral y profesional relacionada del personal de libre nombramiento y remoción, en los términos en que lo establece la mencionada circular.

(OM) A partir de la Auditoría al SGSI 2020, se evidenció que los formatos Anexo Estudios Previos Prestación de Servicios Profesionales y de Apoyo a la Gestión – Análisis de Sector, código 11-01-FR-10 y Matriz de Asignación de Riesgos Previsibles, código 11-01-FR-13, no contemplan específicamente los riesgos de seguridad y privacidad de la información. Igualmente, en el formato Verificación Hoja de Vida, 11-01-FR-15, v. 1,3. no se evidenció un control para la verificación de autenticidad de los soportes aportados por el futuro contratista, por lo que se recomienda ajustar los formatos con el propósito de que se contemplen los riesgos de seguridad de la información puntuales relacionados con las actividades a desarrollar y, se realice la verificación de antecedentes y experiencia profesional con la profundidad requerida dependiendo de las obligaciones del contrato, para evitar la materialización de riesgos, tanto de corrupción como de proceso,

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





relacionados con el manejo de información sensible en la Unidad, y riesgos de contratación por incumplimientos al no tener la idoneidad e integridad requerida para realizar las obligaciones contractuales.

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.

- Para los contratistas de prestación de servicios, persona natural y jurídica, se observó que en el formato Estudios y Documentos Previos Procesos de Contratación Directa, 11-01-FR-04, v. 3.2., hay cláusulas que como "(...) b) *Guardar la debida reserva y confidencialidad de los asuntos que conozca con ocasión de la ejecución del objeto contractual, así como de todos aquellos relacionados con el mismo (...)*", la suscripción del acuerdo de confidencialidad y "(...) d) *En el evento que el contratista para el desarrollo del contrato requiera que la UAECD transmita total o parcialmente bases de datos con datos personales, este deberá cumplir con lo determinado en el "Anexo Compromiso de Confidencialidad en la Transmisión de Datos Personales" (...)*.
- Se evidenció 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 conocer 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.*"

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.

- 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

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

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.”.

- El formato Compromiso de Confidencialidad para el Manejo y Buen Uso de la Información y la Tecnología UAECD, código 05-01-FR-17, es firmado por los servidores públicos (funcionarios provisionales, de carrera administrativa, libre nombramiento y remoción y, contratistas) de la Unidad. Así mismo, como se mencionó en el punto anterior, para los contratistas de prestación de servicios, persona natural y jurídica, se observó que en el formato Estudios y Documentos Previos Procesos de Contratación Directa, 11-01-FR-04, v. 3.2., hay cláusulas que relacionadas con el cumplimiento de lineamientos de seguridad y privacidad de la información.

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.

- Se evidenció el Plan de Sensibilización, Capacitación y Comunicación del Subsistema de Gestión de Seguridad y Privacidad de la Información, vigencia 2020 que contiene, entre otros puntos, las actividades para la gestión de la cultura de seguridad de la información en la Unidad y el cronograma de ejecución de estas. Se revisaron los resultados de las encuestas aplicadas a los funcionarios y contratistas con el fin de evaluar el nivel de conocimiento y la apropiación de las políticas de seguridad de la información, evidenciando que se llevó a cabo en la fecha programada. Igualmente, se evidenciaron las presentaciones realizadas durante el 1er semestre de 2020 en temas referentes al SGSI.
- 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.*
- Se revisaron 18 acuerdos de confidencialidad firmados por personal de planta, recibidos mediante correo electrónico el día 17 de julio de 2020, enviado por la funcionaria de la Subgerencia de Recursos Humanos delegada para atender la presente auditoría.
- Para verificar la apropiación de las socializaciones realizadas con respecto al SGSI y de la documentación publicada en el ISODOC, dentro de la encuesta realizada por el grupo auditor se incluyeron las siguientes preguntas:

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co



 UAECD Catastro Bogotá	INFORME DE EVALUACIÓN Y/O AUDITORÍA DE GESTIÓN DE CONTROL INTERNO
--	--

Pregunta	Respuestas acertadas	Observación OCI
¿Qué entiende por activos de información?	N/A	Aunque el concepto no es igual al planteado en la norma, el personal tiene nociones muy aproximadas a su definición
Nombre un activo de información que gestiona y/o custodia en el proceso al que pertenece:	N/A	Se mencionaron activos sobre los cuales se tienen custodia o responsabilidades dependiendo de las labores que realiza la persona.
¿Qué mecanismos utiliza o conoce para controlar la información clasificada o reservada a su cargo?	N/A	Se reconocen los diferentes mecanismos establecidos: perfiles de acceso, contraseñas, manejo restrictivo de la información, entre otros.
La Política de uso aceptable no aplica para personal externo.	76	
Pregunta	Respuestas acertadas	Observación OCI
¿Qué áreas identifica como "áreas seguras" en la Unidad?		Ninguna persona identificó todas las áreas seguras de la Unidad. Las áreas con mayor reconocimiento fueron: archivos 27, centro de documentación 18, centro de cableado 11, planoteca 4. Se considera que el área donde está ubicada la Gerencia de Tecnología es un área segura (21 respuestas).
Escoja el evento o incidente de seguridad que pueda poner en riesgo la integridad, confidencialidad o disponibilidad de la información en la UAECDC:	86	El 84% del personal reconoció correctamente los incidentes de seguridad.
La política de control de acceso establece que, para el personal externo, el acceso a información y a los recursos tecnológicos deben ser gestionados a través de la Gerencia Comercial y Atención	66	El 64% de los encuestados respondió de manera correcta.
Los contratistas no tienen sanciones por faltas a la seguridad de la información.	98	El 96% de los funcionarios y contratistas saben que estos últimos están sujetos a sanciones por no cumplir las normas de seguridad de la información de la Unidad.
¿Considera Ud. que hace parte activa del Subsistema de Seguridad y Privacidad de la Información?	100	El 98% de los encuestados reconocen que de una y otra forma hacen parte activa del SGSI y tienen responsabilidades frente a él.
Escoja una de las responsabilidades que usted tiene asociada a los dispositivos móviles personales que acceden a la información de la Unidad son:	67	El 65% del personal reconoce que debe proteger la información institucional que manejen en los dispositivos móviles personales.

Se puede concluir que 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 en aprox. el 80%, 20% por encima del que se evidenció el año inmediatamente anterior

Recomendación:

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

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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

- Mediante correo electrónico recibido el día 9 de julio de 2020, la Jefe de la Oficina de Control Disciplinario -OCD- informó que "*Como se aprecia, el no atender los manuales y procedimientos de la Entidad, constituye falta y dentro de esa órbita se asocia el referenciado en su requerimiento, por ello se dejó plasmado que ante los incidentes de seguridad, debía reportarse a la OCD, para que en el ámbito de la competencia y del estudio probatorio se califique la conducta, en términos de tipicidad, ilicitud sustancial y culpabilidad de la conducta.*", entre estos documentos en mención, se encuentra el Documento Técnico de Políticas Detalladas de Seguridad y Privacidad de la Información, entendiéndose que el incumplimiento de este genera las acciones correctivas a que haya lugar.
- Considerando lo anterior, se revisaron los procedimientos: 1. Gestión Disciplinaria, código 15-01-PR-01, 2. Cumplimiento de Sanción Disciplinaria, código 15-01-PR-02, 3. Gestión Preventiva, código 15-01-PR-03, cumpliendo con lo establecido en el control. Así mismo, la Jefe de Control Disciplinario informa que no ha habido procesos relacionados con incumplimientos a la seguridad de la información de junio de 2019 a junio de 2020.
- Teniendo en cuenta que, en la auditoría del año 2019, se evidenciaron falencias en el manejo de las comunicaciones internas que se manejan durante las indagaciones disciplinarias que realiza la OCD, y dado que actualmente la gestión disciplinaria se adelanta de manera virtual, se indagó por la seguridad de la información que manejan las comunicaciones en el Cordis.

En entrevista con el Técnico Operativo 314-05 de la Subgerencia Administrativa y Financiera (encargado de dar soporte operativo del Cordis), se indagó sobre la parametrización que tiene el Cordis en cuanto a las comunicaciones que contienen información reservada como lo son las relacionadas con la Gestión Disciplinaria, estableciendo que las mismas pueden ser vistas en el cordis por todo el personal del área que produce y/o recibe la comunicación, no tiene restricción por usuario productor o receptor de la comunicación y sus anexos. En el gestor de contenidos -WCC- se puede observar tanto la comunicación como sus anexos y a las personas se les da acceso a la a través de uno roles definidos.

Hallazgo:

(AC) A partir de la auditoría al SGSI de la UAECD 2020, se evidenció el incumplimiento de lo 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 digitales remitidos desde y hacia la Oficina de Control Disciplinario a través de la herramienta Cordis, 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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- Se evidenció el Procedimiento Gestionar Retiro de Personal, código 06-01-PR-02, v.4 del 09/10/2019, allí se indica “*ENTREGA DEL CARGO. La Subgerencia de Recursos Humanos informará la novedad de la retiro a la Subgerencia Administrativa y Financiera, a la OAPAP y a la Oficina Jurídica para que se gestionen las actividades asociadas al tema de inventarios, eliminación de claves de acceso a aplicativos y a la Gerencia de Tecnología para la eliminación de usuario: correo, red e impresión. Los jefes de dependencia deben solicitar a través de la mesa de servicios TI la eliminación de claves, permisos y accesos a los aplicativos, para consulta y realización de trámites tanto internos como externos.*”
- En el Procedimiento Gestión de Accesos, código 13-02-PR-04, V.6 del 10/09/2019, 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.
- 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.

- 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, Procedimiento Gestión de Riesgos sobre los Activos en el Marco de la Seguridad de la Información código 02-02-PR-03, 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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

- El procedimiento 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 que conforman la cadena de valor de la Unidad: datos o información, hardware, software, servicios, recurso humano o conocimiento, e instalaciones.
- En la url https://www.catastrobogota.gov.co/instrumentos-de-gestion?field_clasificacion_target_id=175, de la página web de la Unidad, se evidenció la publicación del registro de activos de información vigencia 2019 y se verificó que cada dependencia tiene sus registros de inventario de información siguiendo las indicaciones dadas en el procedimiento mencionado en el ítem anterior. Se tiene previsto realizar la actualización de estos, a más tardar el 31 de agosto según lo aprobado en el plan de acción para la vigencia 2020.

A.8.1.2 Propiedad de los activos

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

- 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.

- 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 aplican 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 (reglas para el uso del correo electrónico, internet, redes sociales) o espacios de participación (foros, chats, blogs, entre otros), sobre el uso del (OneDrive, Teams y Yammer), con parámetros y controles establecidos desde la Gerencia de Tecnología y aplicados a través de la administración de las herramientas antes mencionadas, autorizadas por cada jefe de dependencia.
- Para el caso de los activos que se manejan en los aplicativos, como SIIC, FOCA, etc. se asignan roles y perfiles de acceso a la información, autorizados por el jefe de cada área responsable del activo, según corresponda a las responsabilidades y roles de los funcionarios o contratistas. Para el caso de los activos que se manejan fuera de los aplicativos, se implementan los controles establecidos en los procedimientos que se aplican en cada fase o etapa del proceso. Igualmente, se asignan responsabilidades a los integrantes del equipo en las concertaciones de compromisos y en los contratos que se suscriben, que delimitan el campo de acción. A su vez se aplican controles en el acceso a los archivos de gestión, a los cuales sólo puede ingresar el personal autorizado para dicha labor.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- 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.*
- 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 Subproceso de Gestión de Bienes e Inventarios), código 07-01-PR-02, V.4, 12/02/2020, 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.4.1, 31/01/2020.
- Persiste la observación de la auditoría 2019, en cuanto a que: *“No obstante, existen los documentos antes mencionados, no se evidencia la estrategia de verificación de devolución de los activos de información 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”.*
- Finalmente, no hay claridad en cuanto a qué área debe guardar 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.”.*

(OM) A partir de la auditoría al SGSI de la UAECD 2020, se ratifica la oportunidad de mejora del año 2019, en cuanto a que no se evidencia la estrategia de verificación de devolución de los activos de información físicos, ni para contratistas ni para funcionarios, teniendo en cuenta que este tipo de activos no está incluido en el formato Constancia para Entrega de Bienes y/o Elementos Asignados y Documentos, código 07-01-FR-04, 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).

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- 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.
- En el inventario de activos de información 2019 se evidencia el llenado de las columnas tipo de soporte, tipo de origen, estado y custodia de la información, clasificación del activo en el marco de la seguridad de la información y datos personales, sin embargo, en la columna Clasificación Documental (Categoría de Información) se evidencian casillas "sin establecer".

CUADRO DE CARACTERIZACIÓN DOCUMENTAL																	
Norma, función o proceso	Código del Procedimiento	Tipo documental			Tipo de Soporte (medio de conservación y/o soporte)				Tipo de Origen		Clasificación Documental (Categoría de Información)			Estado y Custodia			
		Nombre del registro o documento de archivo	Definición	Idioma	Análogo	Digital	Electrónico	Descripción del Soporte	Presentación de la información (formato)	Interno	Externo	Serie	Subserie	Descripción de la categoría de información	Custodia de la información	Estado de la información	Localización de la información
109	Disposición de información	05-01-PR-02	Oficio	Recibe solicitud de trámite por parte del cliente	Español	X		Papel	No Aplica	X		Sin establecer	Sin establecer	Sin establecer	GCAU-Gerente	Disponible	archivo de
110	Disposición de información	05-01-PR-02	Oficio	Comunicar al cliente que faltan documentos	Español	X		Papel	No Aplica	X		Sin establecer	Sin establecer	Sin establecer	GCAU-Gerente	Disponible	archivo de
111	Disposición de información	05-01-PR-02	Registro SIC	Verifica que sobre el predio no hay otra solicitud.	Español		X	Disco duro	Base de datos	X		Sin establecer	Sin establecer	Sin establecer	GCAU-Gerente	Disponible	Aplicativo
112	Disposición de información	05-01-PR-02	Oficio	Comunicar al cliente que existe para ese predio otra solicitud	Español	X		Papel	No Aplica	X		Sin establecer	Sin establecer	Sin establecer	GCAU-Gerente	Disponible	archivo de
113	Disposición de información	05-01-PR-02	Comprobante de radicación - oficio	Generación de la radicación en el SIC	Español		X	Disco duro	.PDF	X		Sin establecer	Sin establecer	Sin establecer	Gerencia Tecnología-Gerente	Disponible	Aplicativo
114	Disposición de información	05-01-PR-02	Planilla	Remitir raditaciones a las áreas de estudio	Español	X		Papel	No Aplica	X		Sin establecer	Sin establecer	Sin establecer	GCAU-Gerente	Disponible	archivo de

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.

- La entidad tiene documentado el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, V.6. del 17/07/2020, y en su numeral 3.4. Etiquetado de activos, muestra el esquema de clasificación de acuerdo con los niveles de confidencialidad definidos para la Unidad, tanto para medios electrónicos como físicos de la información.
- 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

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





UAECD
Catastro Bogotá

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

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.

- Se observó que los expedientes documentales, tanto de gestión como archivo central, se han etiquetado de acuerdo con los lineamientos del centro de documentación. Adicionalmente, como producto de la PDA-2019-556 de la auditoría del año 2019, en este momento se está implementando un proceso de depuración de la información del fileservidor con todas las áreas de la entidad, liderado por la Oficial de Seguridad, para incluir el etiquetado de información pública (IP), clasificada (IC) y reservada (IR), el cual se finalizará en el mes de julio de 2020.

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.

- La entidad tiene documentado el Procedimiento Gestión de Activos en el Marco de la Seguridad de la Información, V.6. del 17/07/2020, que da los lineamientos para la creación o modificación del registro de activos de información de la Unidad, ese registro tiene las restricciones de uso o acceso a los activos, así como su clasificación.
- Se cuenta con el Procedimiento Copias de Respaldo y Recuperación, código 13-02-PR-32 del Proceso Provisión y Soporte de Servicios de TI, igualmente con los procedimientos: Organizar Archivos de Gestión, código 08-03-PR-01 y Préstamo y Consulta de Documentos, código 08-03-PR-02 del Proceso de Gestión Documental, que da línea para el manejo de activos de información físicos.
- 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 encuentra en implementación el gestor documental de contenidos (WCC) integrado con el CORDIS.

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 medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

- 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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





- Por otra parte, aunque no hay una política específica para los medios removibles, a lo largo del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, se dan lineamientos para el manejo de estos, por ejemplo, en las políticas de transferencia de información y, política de escritorio y pantalla limpios.
- 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.
- Se evidenció el contrato de prestación de servicios 196-2020, con Transportes Cococarga Ltda., cuyo objeto es “*Servicio de guarda, custodia y transporte de medios magnéticos*”, que inicio el 30/05/2020 y finaliza el 29/05/2021, donde, entre otras, se observa que el proveedor cumple con las disposiciones del Acuerdo 049 de 2000 (del Reglamento General de Archivos sobre “condiciones de edificios y locales destinados a archivos”) y el Acuerdo 008 de 2014 (“Por el cual se establecen las especificaciones técnicas y los requisitos para la prestación de los servicios de depósito, custodia, organización, reprografía y conservación de documentos de archivo y demás procesos de la función archivística en desarrollo de los artículos 13° y 14° y sus parágrafos 1° y 3° de la Ley 594 de 2000”), expedidos por el Archivo General de la Nación - AGN.

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.

- 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 (CD2, DVD3, USB4, Tarjeta de memoria).*”
- 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.
- 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.

³ Disco Versátil Digita - DVD (Por sus siglas en inglés Digital Versatile Disc)

⁴ Bus Universal en Serie - USB (Por sus siglas en inglés Universal Serial Bus)

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90

Código postal: 111311

Torre A Pisos 11 y 12 – Torre B Piso2

Tel: 2347600 – Info: Línea 195

www.catastrobogota.gov.co

Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- 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.

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.

- La entidad tiene documentadas las políticas: 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.
- En correo del 09/07/2020, al indagar sobre ¿qué controles existen para la aplicación y verificación de la Política de control de Acceso, en el caso del trabajo remoto que se ha venido realizando durante la cuarentena por covid.19?, la Oficinal de Seguridad informó que “*Se han realizado depuraciones mensuales y cuatrimestrales. Para el trabajo remoto cada funcionario accede a través de la VPN con su usuario y contraseña. Se realiza el acceso a la VPN mediante las credenciales de red de cada usuario y para algunos casos se cuenta con doble autenticación a través de un token de seguridad que se genera desde un dispositivo físico que tiene el usuario.*”
- Igualmente, la entidad tiene documentado en el Procedimiento Gestión de Accesos, código 13-02-PR-04, V.6, 10/09/2019, asociado al proceso de Provisión y Servicios de TI, el numeral 3.11. Control de acceso a los recursos de red.
- 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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





- 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.
- 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.
- Se evidenciaron correos activos de personal retirado (la mayoría más de 6 meses), se envió un correo de prueba a algunas cuentas de personal que se retiró de la entidad, y no fueron rechazados o devueltos con mensaje de error o de que el personal ya no laboraba en la entidad, no obstante se evidenció la solicitud de desactivación de los usuarios mencionados.

Nota: En mesa de trabajo del día 11 de agosto con la Gerencia de Tecnología, se determinó modificar la oportunidad de mejora como una recomendación, por cuanto lo evidenciado no afecta la seguridad de la información.

Recomendación: A partir de la auditoría al SGSI de la UAECD 2020, se evidenciaron correos de personal retirado desde hace 4 meses o más, que aún aparecen en el directorio de correos de la Unidad, a pesar de sus usuarios fueron desactivados como lo indica el Procedimiento Gestión de Accesos, código 13-02-PR-04, numeral 3.1.1. Novedades de personal y contractuales. Por lo anterior, se sugiere revisar las causas de esta desviación y que no aparezcan como activos o que al momento de enviar un mensaje a estos correos sea devuelto un mensaje indicando que la persona ya no se encuentra vinculada con 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.

- 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 soportan 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.

- Se evidenció 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.*”

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- Se observa en el Procedimiento Gestión de Accesos, código 13-02-PR-04, el numeral 3.6. Depuraciones y Revisiones Periódicas, indica que se deben realizar depuraciones automáticas a los 60 días de inactividad de una cuenta de red o por expiración de una cuenta de un usuario de red, las cuentas de usuario de los sistemas de información se deben depurar mensualmente; así mismo las revisiones de cuentas de usuario y sus privilegios se realizan cuatrimestralmente.
- Se evidenciaron los soportes remitidos por la Subgerente de Infraestructura Tecnológica de la depuración mensual realizada con corte al 31 de mayo 2020 y la cuatrimestral con corte a diciembre de 2019, como se indica en el numeral 3.6. Depuraciones y revisiones periódicas del Procedimiento Gestión de Accesos, código 13-02-PR-04.

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.

- Se evidenció 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 observaron los soportes de mesas de servicio

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





remitidas por la Subgerencia de Recursos Humanos informando el retiro de personal y solicitando la desactivación de sus usuarios, y la depuración de usuario realizada por la Subgerencia de Infraestructura como se mencionó en el numeral A.9.2.5 Revisión de los derechos de acceso de usuarios..

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.

- 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.

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.

- 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 de 2019, 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.

- La entidad tiene documentado el estándar para la 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.

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





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.

- 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.

- 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.

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

A través de correo del 01/07/2020, la Ofical de Seguridad remitió el archivo de Excel “Matrices_Riesgos_SI_DP_UAECD”, el cual por motivos de seguridad no puede ser publicado, en el cual se evidenció que la Unidad cuenta con documentación formal de los riesgos y controles que buscan asegurar los activos de información de la entidad clasificados como críticos (con alto riesgo) y está validado al 11/12/2019 (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 (Captura, Disposición e Integración de la Información, Control Interno Disciplinario, Gestión Contractual, Gestión Documental, Provisión y soporte de servicios de TI y Gestión del Talento Humano).

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co





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 la implementación y aplicación de los mencionados controles.

En cuanto al mapa de riesgos institucional vigente desde diciembre de 2019, se tienen consignados riesgos de corrupción y de proceso relacionados con el manejo de la información con su respectivo plan de tratamiento o manejo de riesgos, a los cuales se les realiza seguimiento trimestral por parte de las áreas y son revisados por la Oficina de Planeación y Aseguramiento de Procesos y verificados por la Oficina de Control Interno.

Teniendo en cuenta las nuevas condiciones de trabajo en casa por cuenta del covid-19, es importante evaluar y controlar los nuevos riesgos que puedan surgir alrededor de la utilización de herramientas e información a través de la conexión remota con la Unidad desde los equipos personales tanto de funcionarios como de contratistas, y cualquier otro tipo de riesgo, de corrupción o proceso, que pueda surgir a raíz del nuevo escenario que está viviendo la entidad.

7. FORTALEZAS.

El Subsistema de Gestión de Seguridad y Privacidad de la Información se encuentra alineado con los objetivos de la UAECD, lo cual convierte a la seguridad en un habilitador de negocio y en un elemento para lograr que los riesgos no se materialicen ni perjudiquen el desarrollo de las actividades que adelanta la entidad tanto internas como externas.

La participación de las áreas y su personal (funcionarios y contratistas) en la aplicación de controles, así como en las sensibilizaciones y capacitaciones realizadas, hacen que el sistema avance en apropiación y por lo tanto su sostenibilidad a mediano plazo pueda ser mantenida. Igualmente, se observaron estrategias, actividades, acciones permanentes que buscan el constante mejoramiento del Subsistema.

8. CONCLUSIONES

Teniendo en cuenta los objetivos de la presente auditoría, en cuanto a verificar el uso y apropiación de los lineamientos definidos para el SGSI en la UAECD y con el alcance de verificar y evaluar el cumplimiento de lo establecido en los controles A.5. a A.9. del Anexo Técnico de la norma ISO 27001:2013, se puede concluir que la entidad tiene documentados e implementados los 39 controles establecidos en la norma, los cuales son susceptibles de mejora teniendo en cuenta los hallazgos registrados a lo largo del presente informe, para los cuales se deberá establecer un plan de mejora.

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

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
 Código postal: 111311
 Torre A Pisos 11 y 12 – Torre B Piso2
 Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
 Trámites en línea: catastroenlinea.catastrobogota.gov.co





9. RECOMENDACIONES

Como resultado de la presente auditoría se encontraron 4 oportunidades de mejora y 2 acciones correctivas. Igualmente, se plantearon 7 recomendaciones a lo largo del informe.

Adicionalmente, se sugiere 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.

Cordialmente,



JOHNY GENDER NAVAS FLORES
Jefe Oficina de Control Interno

Con copia:

- María Clara Rodríguez – Jefe OAPAP
- Helvert Alberto Guzmán – Jefe Oficina Asesora Jurídica
- Mayiver Méndez Sáenz – Jefe Oficina Control Disciplinario
- Hector Henry Pedraza – Gerente de Tecnología
- Luis Javier Clevez – Gerente de Gestión Corporativa
- Rosalbira Forigua – Subgerente de Recursos Humanos

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

Unidad Administrativa Especial de Catastro Distrital

Av. Carrera 30 No. 25 - 90
Código postal: 111311
Torre A Pisos 11 y 12 – Torre B Piso 2
Tel: 2347600 – Info: Línea 195
www.catastrobogota.gov.co
Trámites en línea: catastroenlinea.catastrobogota.gov.co

