



**Comisión
de Regulación
de Agua Potable y
Saneamiento Básico**

INFORME DEFINITIVO DE SEGUIMIENTO AL MAPA DE RIESGOS DE GESTIÓN Y DE SEGURIDAD DIGITAL DE LA UAE-CRA A 31 DE DICIEMBRE DE 2019

1º de Mayo de 2020



**La vivienda y el agua
son de todos**

Minvivienda

OBJETIVO

Verificar la gestión de la UAE CRA respecto al tratamiento de los riesgos de gestión y seguridad digital identificados en la vigencia 2019, en desarrollo del Objetivo Estratégico Quinquenal 2020-2024 "Fortalecer la gestión institucional con base en su independencia y capacidad técnica para que los agentes del sector reconozcan a la entidad, como eficiente, moderna y con un capital humano", y el Proyecto Estratégico "Optimizar la gestión administrativa para apoyar de manera eficiente el logro de las metas institucionales".



CRITERIOS DEL SEGUIMIENTO

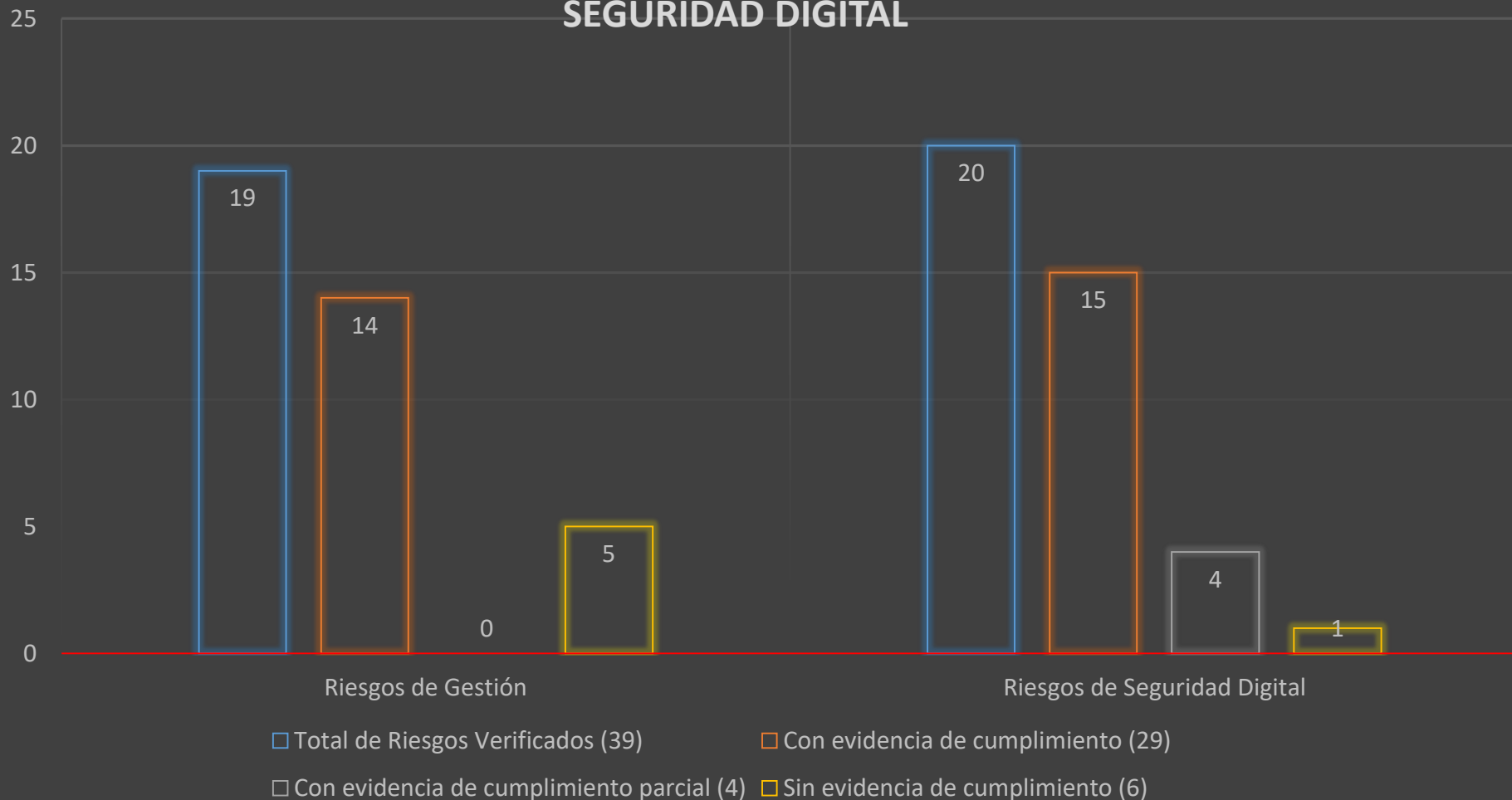
Los criterios observados en el ejercicio del seguimiento fueron:

- Cumplimiento de las acciones de tratamiento previstas para los riesgos de gestión y seguridad digital identificados en el mapa de riesgos de la UAE-CRA a 31 de diciembre de 2019, información obtenida de los registros de la carpetas compartidas de calidad Mapa de riesgos.xlsx y \PLANES CRA 2020\Evidencias Riesgos 31-12-2019.



Seguimiento Riesgos de Gestión y Seguridad Digital a 31 de diciembre de 2019

EVIDENCIA DEL CUMPLIMIENTO DE LOS RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL



Comisión
de Regulación
de Agua Potable y
Saneamiento Básico

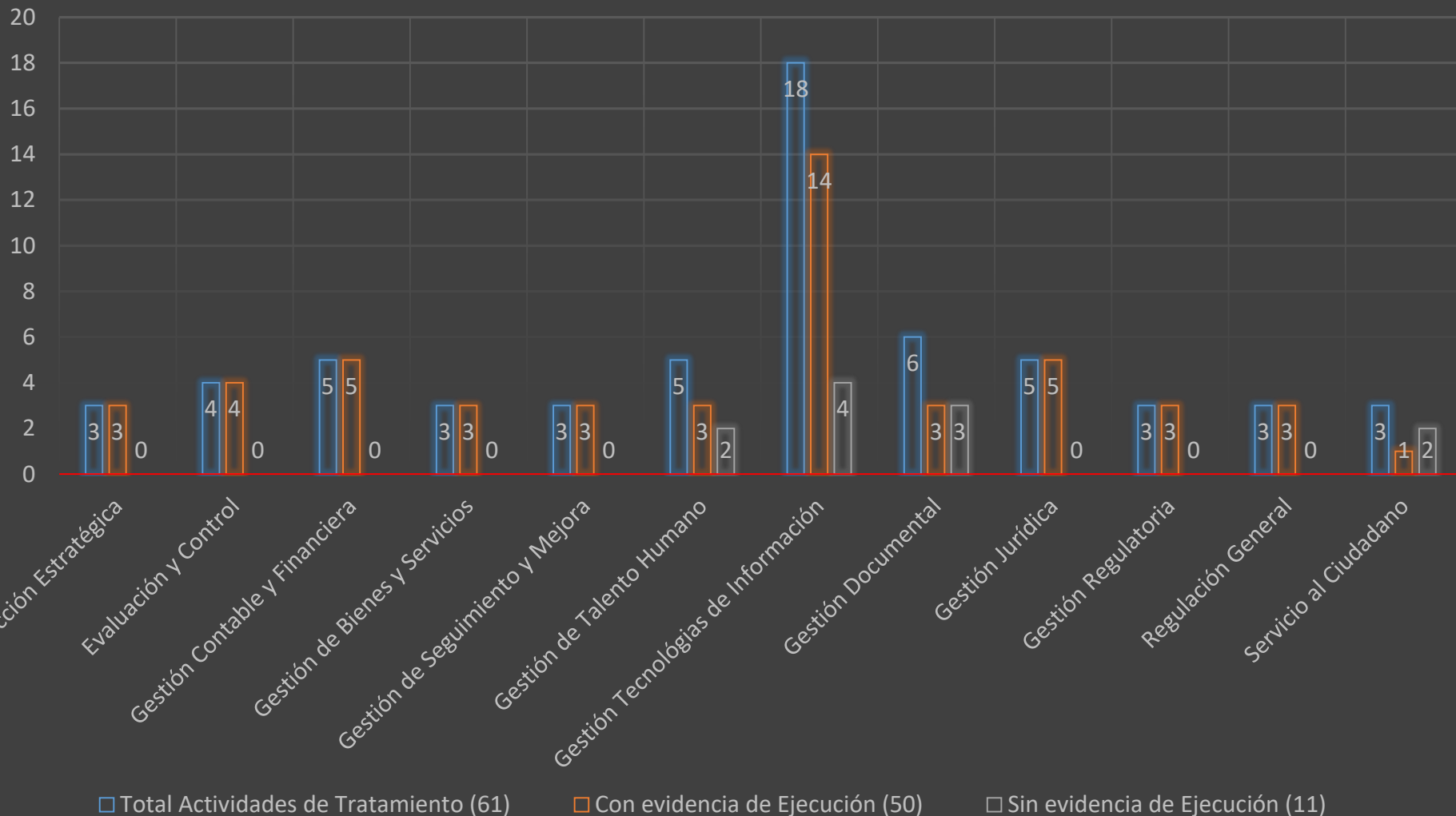


La vivienda y el agua
son de todos

Minvivienda

Seguimiento Riesgos de Gestión y Seguridad Digital a 31 de diciembre de 2019

Actividades de Control



**Comisión
de Regulación
de Agua Potable y
Saneamiento Básico**



**La vivienda y el agua
son de todos**

Minvivienda

Seguimiento Riesgos de Gestión y Seguridad Digital a 31 de diciembre de 2019

Verificación Actividades de Control

✓	Actividades de control con evidencia de ejecución	50
✗	Actividades de control sin evidencia de ejecución	11
Total actividades de control		61



Observaciones y Recomendaciones

- ❑ Una vez verificadas las actividades de control de los riesgos de gestión y de seguridad digital de la vigencia 2019, se evidenció que al 31 de diciembre de ese mismo año se obtuvo un cumplimiento del 82% (50/61).

Este porcentaje es inferior al obtenido en la vigencia 2018, en el que se alcanzó un cumplimiento del 96%, situación que en opinión de esta unidad se originó en que en los tres primeros trimestres del año verificado, no se contaba con un mapa de riesgos consolidado que incluyera las respectivas actividades de control, conforme a lo manifestado por el suscrito en el Comité Institucional de Gestión y Desempeño No 4 del 26 de julio de 2019 y en el Comité de Coordinación del Sistema de Control Interno No 4 del 5 de agosto del mismo año.

- ❑ Dentro del Mapa de riesgos de gestión, de corrupción y de seguridad digital, se evidenciaron dos riesgos del proceso de Gestión Jurídica con las letras (N.A.) en las columnas de “Actividades de control”, y en “Soportes de la actividad de control”; sin embargo, una vez revisadas las evidencias registradas en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se encontró que estos riesgos fueron mitigados de acuerdo a las actividades evidenciadas en la carpeta.



Observaciones y Recomendaciones

- ❑ Dar cumplimiento a las actividades de control previstas en la matriz de riesgos para cada uno de los procesos establecidos en el Sistema de Gestión y Control, permitiendo así el logro de los objetivos propuestos por la entidad para la vigencia.
- ❑ Se recomienda a los líderes de proceso y/o los funcionarios responsables de las actividades de tratamiento, analizar si las actividades programadas para el tratamiento de los riesgos, son eficaces respecto a disminuir o mantener su nivel de exposición, para efectos de revisar, ajustar o reformular los controles de mitigación de aquellos riesgos que son reiterativos en cada vigencia.



ANEXOS



Comisión
de Regulación
de Agua Potable y
Saneamiento Básico



La vivienda y el agua
son de todos

Minvivienda

Riesgo de Gestión	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
Decisiones regulatorias expedidas por fuera de términos y/o con errores. Nombre del proceso: Gestión Regulatoria	Agendar y presentar en Comité de Expertos las decisiones que sean de su competencia.	✓ Correo electrónico de agendamiento a comités de expertos.	Actividad programada según necesidad ✓ Se evidenciaron los correos electrónicos de citación a sesiones de Comités de Expertos de la vigencia 2019.
Representación inadecuada o inoportuna en las actuaciones administrativas o judiciales que se adelanten en contra de la CRA o que ésta deba promover. Nombre del proceso: Gestión jurídica	Revisión y validación de la representación judicial y de la aplicación en ellas de los criterios jurídicos que corresponden.	✓ Informes procesos judiciales.	Actividad programada Mensual ✓ Informes de procesos judiciales radicados en Orfeo de enero a diciembre de 2019. 20190120016043; 20190120016563; 20190120017073; 20190120017433; 20190120018013; 20190120018283; 20190120018933; 20190120019333; 20190120019803; 20190120020553; 20190120020973; 20200120000013
Inadecuada creación y conformación de los expedientes de las actuaciones administrativas a cargo de la Oficina Asesora Jurídica. Nombre del proceso: Gestión jurídica	N/A	N/A	Actividad programada N/A ✓ Se evidenció en el sistema ORFEO el desarrollo para el adecuado manejo de las actuaciones administrativas.
Prescripción de las obligaciones constituidas a favor de la CRA. Nombre del proceso: Gestión jurídica.	N/A	N/A	Actividad programada N/A ✓ De acuerdo a la evidencia que soporta el riesgo, se describe que en el documento GJU- FOR 06 Formato de verificación del expediente, se analiza lo siguiente: 1. Que los títulos estén constituidos de conformidad con la normatividad vigente. 2. Que los títulos ejecutivos contengan una obligación clara, expresa y exigible. 3. Que obre la constancia de notificación y ejecutoria del título ejecutivo. 4. Que obre el estado de cuenta con el saldo de la obligación. 5. En caso de que existan deudores solidarios deberán relacionarse. Su vinculación se efectuará acorde con el Art. 828-1 del E.T. 6. Acreditación o soporte de requerimientos efectuados en etapa de cobro persuasivo. En caso de comunicaciones oficiales se deberán aportar lo certificados de entrega de estas, expedidos por la empresa de correos.
Afectación del PAC e incumplimiento de la circular externa 015 de 12 de mayo de 2017 emitida por el Ministerio de Hacienda y crédito público, frente a la obligación de enviar los formatos diligenciados y firmados. Nombre del proceso: Gestión contable	Correos electrónicos con el archivo adjunto, en el cual se envía formatos diligenciados y firmados con información de SCUN de la Unidad Contable Tesoro Nacional y Explicación Diferencias si las hay.	✓ Correos electrónicos. ✓ Formatos diligenciados y firmados.	Actividad programada mensual ✓ Se evidenció el envío de los correo electrónicos mensualmente con los formatos debidamente diligenciados y firmados a la Unidad Contable del Tesoro Nacional.



Riesgo de Gestión	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
Recaudar un valor inferior al presupuesto establecido para la respectiva vigencia. Nombre del proceso: Gestión contable y Financiera	Se expiden comunicaciones de cobro persuasivo.	✓ Expedientes de Orfeo.	Actividad programada Mensual ✓ Se evidenció en el sistema Orfeo las comunicaciones de cobro persuasivo realizadas por la Subdirección Administrativa y financiera durante la vigencia 2019.
Que no se incluyan todas las transacciones, hechos y operaciones realizados por la entidad en el periodo contable. Nombre del proceso: Gestión Contable y Financiera	Enviar correo electrónico a las distintas áreas involucradas en las transacciones que afectan el proceso contable, con el objetivo de tener la información disponible para garantizar que todas las operaciones llevadas a cabo en la entidad, estén vinculadas en el proceso contable.	✓ Correo electrónico	Actividad programada Mensual ✓ Se evidenció correos electrónicos a diferentes áreas de la UAE-CRA involucradas en el proceso contable.
Evaluación inexistente o inoportuna del Sistema de Control Interno de la UAE CRA. Nombre del proceso: Evaluación y Control	Solicitud escrita, actos administrativos de nombramiento correspondientes.	✓ Solicitud escrita, actos administrativos de nombramiento correspondientes.	Actividad programada al 31/12/2019 ✓ Durante la vigencia 2019, no se reportó ningún caso de ausencia de personal en la Unidad de Control Interno de la UAE CRA que impidiera el cumplimiento del objetivo del proceso.
Inadecuada clasificación y organización documental en el desarrollo de las actividades de gestión documental. Nombre del proceso: Gestión Documental	Realizar capacitación a funcionarios y contratistas, con el objeto de ampliar sus conocimientos en clasificación de documentos.	✓ Material de capacitación / Lista de asistencia.	Actividad programada Semestral ✓ Se evidenció la capacitación de un funcionario de la UAE-CRA, taller denominado " <i>Plan de conservación documental</i> ", igualmente se evidenció el material utilizado en la capacitación.
Pérdida de la información que produce la CRA en formato electrónico. Nombre del proceso: Gestión Documental	Realizar reuniones de trabajo por parte de las áreas con el grupo de gestión documental para establecer el debido manejo que se realizará a los documentos electrónicos que producen.	✗ Listados de asistencia de las reuniones realizadas y las actas del comité de gestión y desempeño donde se aprueban los cambios de los procedimientos. ✗ Crear en el sistema ORFEO los expedientes en los que se custodiara la documentación electrónica .	Actividad programada Semestral Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se anexa un formato en una hoja de Excel con el título de " <i>Revisión de carpetas compartidas</i> " sin diligenciar; igualmente adjuntan correo electrónico en donde envían a revisión el formato de Excel, evidencias que no corresponde al soporte de la actividad de control diseñada para mitigar el riesgo.



Riesgo de Gestión	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
Nombramiento de funcionarios sin el cumplimiento de los requisitos establecidos en el Manual de Funciones y las competencias laborales.	Enviar correo electrónico mensualmente al Subdirector Administrativo y Financiero, evidenciando la revisión o cuando se evidencia alguna falencia o anomalía.	✘ Correo electrónico. ✘ Formato de solicitud de actualización de documentos código GSM-FOR04.	Actividad programada Semestral Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, no se evidenció el soporte de la actividad de control diseñada para mitigar el riesgo.
Incumplimiento de la normatividad en materia de talento humano desarrollo de actividades de bienestar, Capacitación, estímulos y de seguridad y salud en el trabajo.	Realizar sensibilización a los funcionarios en la participación activa que deben tener en las actividades de capacitación, bienestar, incentivos y seguridad y salud en el trabajo.	✓ Listas de asistencia, material de divulgación.	Actividad programada Semestral ✓ Se evidenció las listas de asistencias a las diferentes actividades de capacitación, incentivos y seguridad y salud en el trabajo, igualmente el material de la divulgación de las actividades, del mismo modo se anexa la auditoría de la implementación y mantenimiento del Sistema de Gestión de Seguridad y Salud en el Trabajo de la UAE-CRA.
Errores en la liquidación de nómina y parafiscales.	Se realiza verificación aleatoria por cargos, para identificar que se efectúen los pagos y los descuentos de conformidad.	✘ Correo electrónico a cada funcionario involucrado en el proceso de la nómina.	Actividad programada Mensual Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, no se evidenció el soporte de la actividad de control diseñada para mitigar el riesgo.
Incumplimiento de la Agenda Regulatoria Indicativa.	Realizar seguimiento a través del PAI	✓ PAI y soportes al mismo.	Actividad programada Mensual ✓ Se evidenció el diligenciamiento mensual del avance cualitativo de las actividades programadas en el PAI 2019 por parte de la Oficina Asesora Jurídica, igualmente se evidenció los soportes en aquellas actividades que lo requerían.
Incumplimiento de las actividades del plan de mejoramiento institucional.	Solicitar seguimiento semestral a los líderes de proceso a través de correo electrónico.	✓ Correo electrónico . ✓ Matriz de seguimiento diligenciada	Actividad programada Semestral ✓ Con fecha 13 de enero de 2020, la Oficina Asesora de Planeación y TIC's, solicitó a los líderes de los procesos diligenciar el Plan de Mejoramiento de las Acciones Correctivas y de Mejora. ✓ Matriz de seguimiento diligenciada .



Riesgo de Gestión	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
<p>Incumplimiento de las metas del Plan institucional.</p> <p>Nombre del proceso: Dirección Estratégica</p>	Realizar seguimiento al cumplimiento del PAI trimestralmente.	✓ PAI en Excel con el avance y seguimiento	<p>Actividad programada Trimestral</p> <p>✓ La Oficina Asesora de Planeación y TIC's realizó trimestralmente los seguimientos al Plan Anual Institucional 2019, PAI que se encuentra diligenciado en archivo Excel.</p>
<p>Indebida verificación de los requisitos que se requieren para adelantar en los distintos procesos de contratación.</p> <p>Nombre del proceso: Gestión de Bienes</p>	Emitir alertas en el Comité de contratación sobre el seguimiento al cumplimiento del Plan Anual de Adquisiciones de la entidad.	✓ Acta del comité de contratación.	<p>Actividad programada En los comités de contratación donde eventualmente se trate del tema.</p> <p>✓ Durante la vigencia 2019 se evidenció que el Comité de Contratación de la UAE-CRA se reunió en 43 oportunidades, dando así cumplimiento al plan de anual de adquisiciones.</p>
<p>Reiterativa generación de requerimientos en GLPI por la misma causa, al no identificar la causa raíz de los mismos.</p> <p>Nombre del proceso: Gestión de Tecnologías de Información</p>	Realizar plan de mejoramiento, en donde se consolide las incidencias similares, con el fin de identificar la causa raíz, seguimiento y la efectividad de estas incidencias.	✗ Plan de mejoramiento	<p>Actividad programada Trimestral</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se adjuntó el reporte de la consolidación de las incidencias presentadas durante el mes de diciembre de 2019, no se evidenció el soporte de la actividad de control descrita para mitigar el riesgo.</p>
<p>Incumplir los tiempos de respuesta de las PQRSD establecidos en la normatividad.</p> <p>Nombre del proceso: Servicio al Ciudadano</p>	Realizar capacitación a los servidores de la entidad, con el fin de dar a conocer la importancia del cumplimiento del debido protocolo de atención al ciudadano.	<p>✗ Lista de asistencia.</p> <p>✗ Material de la capacitación.</p>	<p>Actividad programada Anual</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se adjuntó los informes trimestrales de las PQRSD durante la vigencia 2019, no se evidenció el soporte de la actividad de control descrita para mitigar el riesgo.</p>



Riesgo de Seguridad Digital	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
<p>Perdida en la confidencialidad por Fallas en la custodia y manejo de información reservada o pública clasificada relacionada con defensa judicial y cobro coactivo.</p> <p>Nombre del proceso: Gestión Jurídica</p>	<p>1. Realizar inspección de solitudes de la mesa de servicio. 2. Verificar accesos de usuarios en los directorios o activos donde se realiza el almacenamiento.</p>	<p>✓ Numero de ticket o solicitud de la mesa de servicio</p> <p>✓ Bitácora de Permisos de usuarios</p>	<p>Actividad programada a demanda</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios.</p>
<p>Pérdida de la Integridad electrónica relacionada con las Resoluciones de Carácter Particular.</p> <p>Nombre del proceso: Gestión Regulatoria</p>	<p>1. Verificar el acceso a los activos de información que contienen información de resoluciones particulares de manera periódica. 2. Verificar el acceso, y la integridad de la información contenida en el SUI y/o Sinfonía y/o otras fuentes.</p>	<p>✓ Realizar el procedimiento de Gestión de los indicadores de localidad de datos.</p> <p>✓ formato de solicitud de datos</p>	<p>Actividad programada a demanda</p> <p>✓ Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció el procedimiento de Gestión de los indicadores de calidad de datos GTI-PRC06, igualmente se evidenció el formato de Solicitud de datos GTI-FOR06.</p>
<p>Escalamiento de privilegios a servidores por Infección de Virus Ingeniería Social.</p> <p>Nombre del proceso: Gestión de Tecnologías de Información</p>	<p>1. Realizar Validación de Usuarios</p> <p>2. Aplicar reglas de seguridad en la Infraestructura</p>	<p>✓ Formato Registro de Usuarios y Permisos.</p> <p>✓ Documento de informe de vulnerabilidades.</p>	<p>Actividad programada al 31/01/2020</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció un archivo de Excel con los registros de usuarios y permisos de las solicitudes generadas a la mesa de servicio, del mismo modo se evidenció el informe de vulnerabilidades.</p>
<p>Pérdida de disponibilidad de Servicios TIC.</p> <p>Nombre del proceso: Gestión de Tecnologías de Información</p>	<p>1. Verificar la ejecución de las actividades del plan y mantenerlo actualizado</p> <p>2. Verificar la existencia del control de cambios en la mesa de servicio, con su respectiva aprobación.</p>	<p>✗ Informe de ejecución del plan recuperación ante desastre.</p> <p>✗ Formatos de Control de Cambios</p>	<p>Actividad programada Anual</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se adjuntó tres carpetas con diferentes documentos y dos archivos en bloc de notas con los nombres de "Formato de Control de Cambios y el Informe Final de RDP", archivos que se encuentran sin información (en blanco), dentro de las carpetas no se encuentran los soportes de la actividad de control diseñada para mitigar el riesgo.</p>
<p>Pérdida de confidencialidad de información reservada o pública clasificada de la entidad.</p> <p>Nombre del proceso: Gestión Documental</p>	<p>1. Realizar socialización del guía GDO-GUI04 Guía Valoración de Activos V01</p> <p>2. Realizar Registro de la matriz de activos de información</p>	<p>✗ Acta de Socialización de Guía Valoración de Activos V01</p> <p>✓ Matriz de activos de información</p>	<p>Actividad programada Anual</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció la matriz de activos de información, respecto al Acta de Socialización de Guía Valoración de Activos, el archivo adjunto es un bloc de notas el cual se encuentra sin información.</p>



Riesgo de Seguridad Digital	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
<p>Pérdida de confidencialidad de información reservada o pública clasificada de talento humano.</p> <p>Nombre del proceso: Gestión de Talento Humano</p>	<p>1. Realizar la clasificación de la carpeta física de cada funcionario</p> <p>2. Validar y solicitar la clasificación de documentación frente a la privacidad e intimidad dentro del SGD Orfeo</p>	<p>✓ Bitácora de registro de carpetas revisadas</p> <p>✓ Orfeo clasificados correctamente</p>	<p>Actividad programada a demanda</p> <p>✓ Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció el archivo en Excel de la Bitácora de registro de carpetas revisadas y un archivo de Excel de los Orfeos clasificados correctamente.</p>
<p>Falta de oportunidad para localizar información de la entidad en medios electrónicos.</p> <p>Nombre del proceso: Gestión Documental</p>	<p>1. Realizar la clasificación de documentos electrónicos en la matriz de activos de información</p> <p>2. Socializar el procedimiento de información compartida o enviada electrónicamente por terceros</p>	<p>✓ Matriz de activos información</p> <p>✗ Registro de socialización del procedimiento de información compartida o enviada electrónicamente por terceros.</p>	<p>Actividad programada anual</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció la matriz de activos de información. El Registro de socialización del procedimiento de información compartida se encuentra en un archivo de bloc de notas el cual se encuentra sin información.</p>
<p>Pérdida de confidencialidad de información reservada o pública clasificada relacionada con servicio al ciudadano.</p> <p>Nombre del proceso: Servicio al Ciudadano</p>	<p>1. Realizar el registro de la matriz de activos de información</p> <p>2. Realizar sensibilización de datos personales</p>	<p>✓ Matriz de activos de información.</p> <p>✗ Registro de asistencia de sensibilización de datos personales.</p>	<p>Actividad programada anual</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció la matriz de activos de información. El Registro de socialización del procedimiento de información compartida se encuentra en un archivo de bloc de notas el cual se encuentra sin información.</p>
<p>Pérdida de información electrónica relacionada con las actividades de la Agenda Regulatoria Indicativa.</p> <p>Nombre del proceso: Gestión Jurídica</p>	<p>1. Realizar inspección de solitudes de la mesa de servicio. 2. Verificar accesos de usuarios en los directorios o activos donde se realiza el almacenamiento.</p>	<p>✓ Numero de ticket o solicitud de la mesa de servicio.</p> <p>✓ Bitácora de permisos de usuarios a directorios o activos donde se realiza el almacenamiento.</p>	<p>Actividad programada a demanda</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios.</p>
<p>Pérdida de disponibilidad de Información electrónica relacionada con el proceso de gestión de seguimiento y mejora.</p> <p>Nombre del proceso: Gestión de Seguimiento y Mejora</p>	<p>1. Informar al equipo de infraestructura tecnológica los permisos y/o revocación de usuarios a las carpetas o directorios de calidad.</p> <p>2. Realizar backup de la carpeta de calidad según las directrices del procedimiento de backup</p>	<p>✓ Numero de Ticket o solicitud de mesa de servicios</p> <p>✓ Logs de backup</p>	<p>Actividad programada a demanda</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup.</p>



Riesgo de Seguridad Digital	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
<p>Pérdida de Información electrónica relacionada con la planeación institucional.</p> <p>Nombre del proceso: Dirección Estratégica</p>	<p>1. Informar al equipo de infraestructura tecnológica los permisos y/o revocación de usuarios a las carpetas o directorios de calidad.</p> <p>2. Realizar backup de la carpeta de calidad según las directrices del procedimiento de backup</p>	<p>✓ Numero de Ticket o solicitud de mesa de servicios</p> <p>✓ Logs de backup</p>	<p>Actividad programada a demanda</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup.</p>
<p>Pérdida de confidencialidad de información reservada o pública clasificada relacionada con el proceso de evaluación y control</p> <p>Nombre del proceso: Evaluación y Control</p>	<p>1. Aplicar GPO de bloqueo de PC</p> <p>2. Realizar backup de equipos de control Interno</p> <p>3. Aplicar GPO para cambio de contraseña cada 60 días, de mínimo 8 caracteres</p>	<p>✓ Validación de la Política Directorio activo de cambio de claves y bloqueo de estación de trabajo.</p> <p>✓ Logs de ejecución de backups</p>	<p>Actividad programada a 31/12/2019</p> <p>✓ Bloqueo automático del computadores de la Unidad de Control Interno por inactividad durante los últimos cinco minutos. De igual forma, el sistema solicita cambio de contraseña cada 60 días de manera automática, por lo que se protege la confidencialidad de documentos en construcción y de papeles de trabajo que soportan las auditorías de gestión y seguimientos.</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup.</p>
<p>Pérdida de confidencialidad de información reservada o pública clasificada relacionada con las actividades de contratación y/o supervisión.</p> <p>Nombre del proceso: Gestión de Bienes y Servicios</p>	<p>1. Informar al equipo de infraestructura tecnológica los permisos y/o revocación de usuarios a las carpetas o directorios de calidad.</p> <p>2. Hacer firmar a los contratistas acuerdos de confidencialidad</p>	<p>✓ Numero de Ticket o de solicitud y/o Expediente del contrato</p> <p>✓ Validación de Acuerdos de confiabilidad de contratistas</p>	<p>Actividad programada a 31/12/2019</p> <p>✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup. Se evidenciaron 14 acuerdos de confidencialidad de contratistas de la UAE-CRA durante la vigencia 2019.</p>



Riesgo de Seguridad Digital	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
Dificultad y/o falta de oportunidad para localizar información en medios físicos o electrónicos relacionados con contabilidad. Nombre del proceso: Gestión Contable y Financiera	1.Registrar en la matriz nuevos activos de información tema contable 2. Realizar seguimiento a la información compartida o enviada electrónicamente por terceros	✓ Matriz de activos de Información ✓ Registro de actividades de contratistas.	Actividad programada a 31/12/2019 ✓ Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció los archivos de matriz de activos de información y el registro de actividades de contratistas de la UAE-CRA.
Pérdida en la Disponibilidad electrónica relacionada con las actividades de la Agenda Regulatoria Indicativa. Nombre del proceso: Regulación General	1. Registrar nuevos activos en la matriz activos de información 2. Asignar y/o revocar permisos de acceso a directorio y/o archivos.	✓ Matriz de activos de información. ✓ Bitácora de permisos de carpetas o directorios	Actividad programada a 31/12/2019 ✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup. Igualmente se evidenció la matriz de activos de información.
Perdida de la Disponibilidad en Servidores de virtualización ORACLE. Nombre del proceso: Gestión de Tecnologías de Información	1. Generar backup de maquinas virtuales 2. Registro Vitacura de acceso a Datacenter / 3. Bitácoras de entrega de medios a tercero contratado.	✓ Log de backup ✓ Bitácora de acceso a Datacenter ✓ Bitácora entrega medios a terceros contratados	Actividad programada a demanda ✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup.
Pérdida de la Disponibilidad en la RED Nombre del proceso: Gestión de Tecnologías de Información	1. Mantener vigente el contrato del servicio de firewall 2. Verificar la actualización de la base de datos del dispositivo y Agrade del firmware 3. Aplicación de políticas en el firewall	✓ Contrato de servicios de Firewall ✓ Pantallazos actualización del firewall y Upgrade del Firmware si aplica. ✓ Reglas de Firewall	Actividad programada Mensual ✓ Se evidenció que el contrato N° 140 de 2018 correspondiente a servicios de Firewall se encontraba vigente a fecha 31 de diciembre de 2019. El Documento de Actualización Firmware Firewall Movistar y el documento de Reglas de Firewall.
Pérdida de la Confidencialidad, Integridad frente a la conectividad remota. Nombre del proceso: Gestión de Tecnologías de Información	1.Realizar validación de usuarios VPN activos en el firewall 2. Registro solicitudes en el GPLI de la activación o desactivación de la VPN	✓ Bitácora de usuarios VPN ✓ Respuesta de ticket de activación o desactivación de VPN.	Actividad programada Semestral ✓ De acuerdo al reporte generado por la Oficina asesora de Planeación y TIC's, se evidenció las solicitudes generadas a la mesa de servicio y la bitácora de permisos de los usuarios y los Logs de Backup.



Riesgo de Seguridad Digital	Actividades de Control	Soporte de la actividad de control	Verificación Unidad Control Interno
<p>Perdida de la Disponibilidad a información alojada en almacenamiento NAS/SAN.</p> <p>Nombre del proceso: Gestión de Tecnologías de Información</p>	<ol style="list-style-type: none"> 1. Realizar borrado seguro de almacenamiento de servidores y equipos de computo 2. Realizar Mantenimiento o garantía de UPS 3. Realizar cambio de cableado a infraestructura y equipos de usuarios local 	<ul style="list-style-type: none"> ✓ Bitácora borrado seguro de almacenamiento de servidores y equipos de computo ✓ Contratos de Mantenimiento y/o Garantía de UPS ✓ Bitácora de cambio de cableado de datacenter y/ de equipos de usuarios locales 	<p>Actividad programada Anual</p> <ul style="list-style-type: none"> ✓ Se evidenció la bitácora de borrado seguro de los equipos de computo que fueron dados de baja en la vigencia 2019, ✓ Se evidencio los contratos N°. 51,52 y 90 de 2019 relacionados con el mantenimiento de UPS y de cambio de cableado a infraestructura y equipos de usuarios locales.
<p>Perdida de la Integridad de Aplicaciones Web</p> <p>Nombre del proceso: Gestión de Tecnologías de Información</p>	<ol style="list-style-type: none"> 1. Realizar Test de código frente a la evaluación de código seguro establecidos por la CRA y/o Control de Cambios 2. Revisión de buenas practicas de la industria frente a desarrollo seguros y adoptados por el tercero 	<ul style="list-style-type: none"> ✗ Test realizados frente a la evaluación de código seguro establecidos por la CRA y/o control de cambios ✓ Documento buenas practicas de desarrollo seguro realizadas por el tercero 	<p>Actividad programada a demanda</p> <p>Dentro de las evidencias o soportes registrados en V:\PLANES CRA 2020\Evidencias Riesgos 31-12-2019, se evidenció el link http://192.168.100.38/gitlab/snippets/2#buenas-pr%C3%81cticas-para-el-desarrollo-seguro el documento de buenas practicas de desarrollo seguro realizado por el tercero. El test frente a la evaluación de código seguro establecido por la UAE-CRA no se evidenció.</p>



Comisión
de Regulación
de Agua Potable y
Saneamiento Básico

GIOVANNI SOTO CAGUA

Asesor con funciones de Control Interno



La vivienda y el agua
son de todos

Minvivienda