SECRETARIA DISTRITAL DE MOVILIDAD

OFICINA DE CONTROL INTERNO

Informe de Seguimiento Decreto 491 de 2020 / Decreto 1078 de 2015 - Continuidad de Negocio (OTIC)

Julio de 2020

MARCO LEGAL:

- Decreto 491 de 2020 “Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica”
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario de Sector de Tecnologías de la Información y las Comunicaciones"
- Manual de Gobierno Digital
- Guía 10 para la preparación de las TIC para la continuidad del negocio (MINTIC – Vive Digital Colombia)

OBJETIVO DEL INFORME:

Evaluar la capacidad de la Secretaría Distrital de Movilidad (SDM) de mantener la operación de la entidad bajo las nuevas condiciones que le impone la contingencia por el COVID 19 y verificar los controles establecidos para llevar a cabo las acciones implementadas.

RESUMEN:

De acuerdo a lo observado por el equipo auditor en el desarrollo del presente seguimiento, una vez evaluadas las evidencias aportadas y la información dispuesta por la entidad tanto en su página web como en la intranet, se evidencia que de manera general la Secretaría Distrital de Movilidad adoptó medidas tecnológicas inmediatas en el marco del Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, que le permitieron dar continuidad a la gestión adelantada por los servidores de la misma, para el desarrollo de sus funciones u obligaciones; lo que a su vez garantizó la continuidad en la atención a la ciudadanía.

No obstante lo anterior, si bien la entidad ha realizado esfuerzos respecto a la respuesta de la misma ante situaciones como las que hoy nos atañe (situación epidemiológica Covid 19), es importante destacar que desde la vigencia 2018 la OCI ha venido recomendando dar continuidad a la implementación del DRP (Plan de Recuperación antes Desastres) de conformidad con el resultado de la evaluación realizada en ese momento a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

En tal sentido se configuró una No Conformidad así:

NO CONFORMIDAD 01:

La entidad no ha dado cumplimiento integral a lo dispuesto en el Artículo 2.2.9.1.2.1 del Decreto 1008 de 2018 y 2.2.17.4.7 del Decreto 620 de 2020; así como lo establecido en la ISO 27001:2013 Anexo A.17; particularmente en lo que tiene que ver con aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: referidos a la planificación de continuidad de negocio.

Aunado a lo anterior se recomienda tener en cuenta las Observaciones y Recomendaciones efectuadas por el equipo auditor de la OCI como resultado del presente seguimiento.

A continuación, se presenta el desarrollo del seguimiento realizado que incluye la gestión llevada a cabo por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), los avances y proyecciones para asegurar la continuidad de la gestión desde el aspecto tecnológico.

DESARROLLO DEL INFORME[1]:

La Oficina de Control Interno (OCI), actuando bajo un enfoque preventivo, según lo establecido en el Decreto 648 de 2017, los lineamientos del DAFP y teniendo en cuenta que la contingencia por el COVID-19 trajo consigo nuevas formas de interactuar frente a los ciudadanos y ha facilitado el trabajo en casa y el teletrabajo haciendo uso de las TIC como estrategia para el cumplimiento de las funciones propias de la Secretaría; consideró relevante verificar la respuesta de la entidad frente a los aspectos más relevantes establecidos por el gobierno nacional y el distrito con el fin de dar continuidad al cumplimiento misional de la SDM.

En tal sentido, a través del radicado SDM-OCI-78841-2020 de fecha 21 de mayo, se solicita a la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), indicar la gestión adelantada debidamente soportada, sobre los temas que a continuación se desarrollan. Respuesta que fue entregada por la OTIC por medio del radicado SDM-OTIC-82147–2020 de fecha 29 de mayo de 2020:

i) Que medidas se han tomado en la Secretaria para garantizar la seguridad y autenticidad de la información, con el fin de dar continuidad a los temas de conciliación y otros mecanismos de resolución de conflictos por medios virtuales, tal y como lo establece al parágrafo 1 del artículo 10 del Decreto 491 de 2020.

Respuesta OTIC:

Atendiendo la circular 005 de 2020 de la oficina del despacho que tiene como asunto MEDIDAS TEMPORALES PARA GESTIÓN DE LOS DIFERENTES TRÁMITES ADMINISTRATIVOS Y FINANCIEROS CON OCASIÓN A LA SITUACIÓN EPIDEMIOLÓGICA (COVID-19), se recomendó a los colaboradores directos e indirectos de la Secretaría Distrital de Movilidad evitar tener contacto con documentos en físico, por tal motivo se deberán adelantar los diferentes trámites de gestión de manera digital.

En consecuencia, a partir del 20 de marzo de 2020, todos los vistos buenos deberán ser tramitados por correo electrónico; por este medio también se emitirá la aprobación de los diferentes documentos por parte de cada una de las personas que intervengan en la construcción del mismo.

Para dar solución a este punto la OTIC realizó la implementación de firma digital de documentos, esto utilizando una entidad certificadora local (*servidor emisor de certificados para el dominio*

[1] En este acápite se debe analizar los posibles riesgos que afecten el tema evaluado.

movilidadbogota.gov.co). La firma digital asegura la identidad, es decir, que el individuo es quien dice ser, o lo que es lo mismo, la autenticación. También se consigue la integridad del documento que está firmado, se asegura que está completo y no ha sido modificado. Y, por último, el "no repudio", porque la persona no puede decir que no es quien es.

Para el manejo de la gestión documental y el uso de aplicativos especiales de la entidad se implementaron manuales, instructivos para el uso de la VPN, como también implementación de herramientas de soporte remoto como AnyDesk.

Se crearon correos en las dependencias para el trámite de correspondencia ordinaria de la SDM y para la atención de tutelas, derechos de petición, entes de control y correspondencia urgente como radicacion@movilidadbogota.gov.co. ventanillacorrespondencia@movilidadbogota.gov.co

Para la radicación de cuentas de los contratistas en la subdirección financiera se creó la ventanilla virtual formulario que debe diligenciar únicamente el supervisor del contrato y permite la radicación de estas.

Para las videoconferencias, video llamadas, reuniones virtuales, comités utilizados en la entidad se encuentra habilitada para todas las cuentas de los usuarios la plataforma meet de Google que permiten prestar los servicios por este medio tecnológico y de comunicaciones.

Para el agendamiento de la orden de entrega de vehículos inmovilizados y salida de patios se implementó un formulario web para facilidad de los ciudadanos.

Para el agendamiento para facilidades de pagos e información de acuerdos de pago se publicó una la página web de la entidad un formulario virtual para facilidad de los ciudadanos.

Se realizó optimización del sistema de publicaciones en el portal web para todas las dependencias de la entidad.

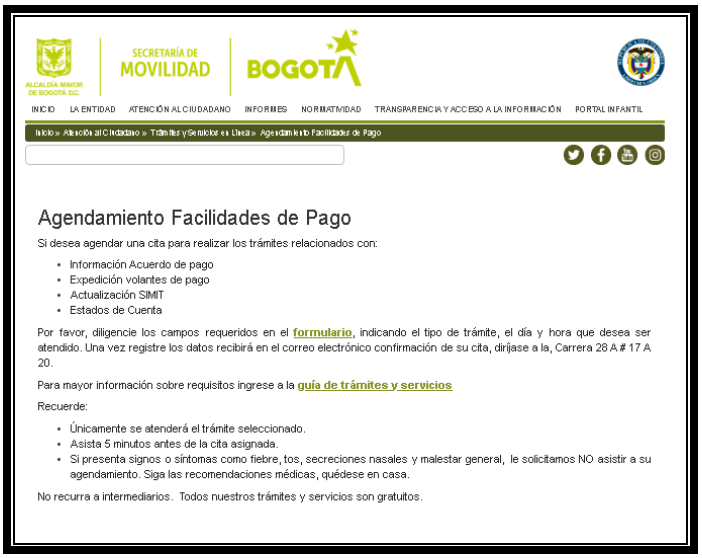
Se realizó optimización de carpetas compartidas en Google drive de todas las dependencias de la entidad en el cual se encuentra toda la documentación emitida como archivo digital.

Verificación de la OCI:

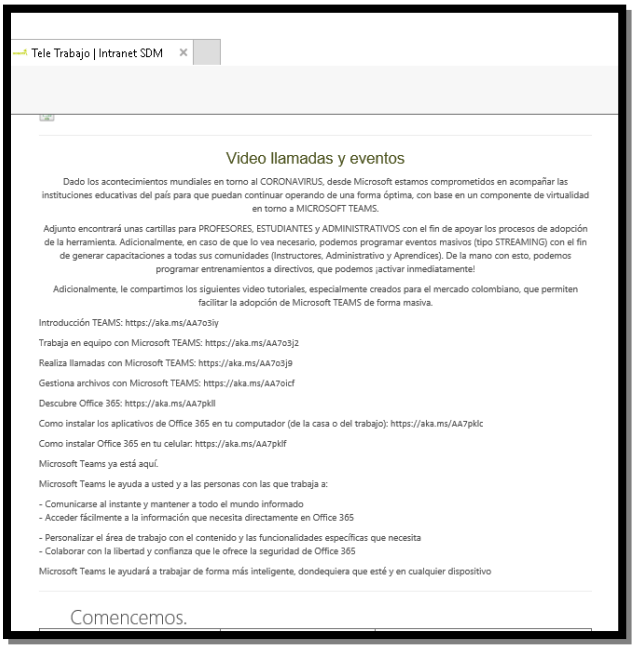
De la verificación realizada a la información publicada en la página web de la entidad se observa:

- ✓ Agendamiento de la orden de entrega de vehículos inmovilizados: (https://www.movilidadbogota.gov.co/web/inmovilizados)

- ✓ Facilidades de pago: (https://www.movilidadbogota.gov.co/web/agendamiento_facilidades_de_pago)



Con relación a la implementación de manuales, instructivos para el uso de la VPN y la implementación de herramientas para llevar a cabo videoconferencias, video llamadas, reuniones virtuales, se observa la siguiente información publicada en la intranet de la entidad (https://intranetmovilidad.movilidadbogota.gov.co/intranet/2020-03-18/tele-trabajo):



Adicionalmente a través de la mesa de trabajo realizada el 11/06/2020 entre el equipo auditor y el equipo de la OTIC que está atendiendo el seguimiento, se aclararon los siguientes aspectos:

- Se crearon correos para el Despacho.
- Toda la correspondencia debe salir de las personas asignadas en cada dependencia.
- Para el ingreso se crearon correos específicos de entes de control.
- Para la empresa de correspondencia 4/72 se crearon correos para ingreso y salida, entre otros.
- Todo se direcciona desde los correos que se asignaron en cada dependencia.

Esta gestión se llevó a cabo de manera conjunta con la Subdirección Administrativa; la OTIC facilitó los medios de acuerdo a lo indicado en la mesa de trabajo

Respecto a la optimización del sistema de publicaciones en el portal web para todas las dependencias de la entidad, se realizan las siguientes precisiones:

- Todas las publicaciones se coordinan con la Oficina Asesora de Comunicaciones y Cultura para la Movilidad de acuerdo a los protocolos.
- Las publicaciones en Intranet se hacen a través de la mesa de servicios previa autorización de la Oficina Asesora de Comunicaciones y Cultura para la Movilidad.

Por último y en relación con las medidas adoptadas por la entidad para garantizar el trabajo en casa y el apoyo brindado para garantizar a su vez la custodia de la información generada en este periodo de confinamiento, se indica:

- Utilización de herramientas para el trabajo en casa como chatbot (movichat) para agilizar los procesos de interacción entre los servidores de la entidad y la mesa de ayuda, tanto para temas generales como específicos.
- Otras herramientas son el chat del correo institucional (hangout) como medio de comunicación con la mesa de servicios y auto consulta (app).
- Se puede utilizar cualquier canal de comunicación para todos los casos.
- Por cualquier medio se asigna número de requerimiento.
- Respecto a la optimización de las carpetas compartidas en Google Drive la capacidad es ilimitada para los usuarios que tienen cuenta de correo corporativo; no hay restricción de capacidad; las anteriores medidas se tomaron como medida de continuidad y para ir introduciendo la utilización de trabajo desde el drive.
- La información de usuarios se puede manejar desde Google Drive.
- La información de Google Drive que no es compartida con otros usuarios, cada usuario la puede ir depurando.
- Cada cuenta de Google Drive tiene su respaldo incorporado en el componente Vault de Google Suite, el cual permite conservar, bloquear, buscar y exportar datos para responder a las necesidades de conservación (definidas por la Entidad) y control electrónico de información dentro de la plataforma y de acuerdo a las políticas de Google.

Se aporta la evidencia de la socialización realizada al interior de la entidad de estas herramientas y la estadística de los medios de comunicación de atención a la mesa de ayuda, en donde se observa que en marzo, abril y mayo el canal más utilizado fue el de correo electrónico, seguido por el canal telefónico.

ii) En virtud de lo establecido en el artículo 11 del Decreto Legislativo 491 de 2020, que medidas ha tomado la Secretaria para *"... garantizar la seguridad de los documentos que se firmen por este medio*." (firma autógrafa mecánica, digitalizadas o escaneadas).

Respuesta OTIC:

Atendiendo la circular 006 de 2020 de la oficina del despacho con asunto MEDIDAS TEMPORALES PARA GESTIÓN DE LOS DIFERENTES TRÁMITES DE LA SDM CON OCASIÓN A LA SITUACIÓN EPIDEMIOLÓGICA (COVID-19), para la suscripción de documentos, la entidad maneja dos tipos de firma digital, una para los ordenadores del gasto, jefes de dependencia y autoridades de tránsito a través de una Entidad de Certificación Digital acredita por la ONAC, el cual es un certificado digital en un archivo informático al que se le asocia los datos de identidad de un suscriptor (persona natural o jurídica) que al momento de ser usado para firmar transacciones electrónicas, garantiza la identidad de quien firma además de integridad y no repudio de la información.

La otra forma se trata certificado digital privado para firma que se puede realizar a través de un enlace disponible en la intranet PKI interna integrada a Directorio Activo, una vez aprobado por la

OTIC se procede a realizar la emisión. Se creó un procedimiento y guía de instalación del certificado y firma de documentos.

Verificación de la OCI:

Sobre esta gestión, la OTIC aclara en la mesa de trabajo que el procedimiento y guía de instalación corresponde al documento PA04-PR02 FIRMA DIGITAL Versión 1 de 18/2/2019 publicado en la Intranet de la entidad y que de conformidad con su fecha de actualización no es un procedimiento nuevo en la entidad.

Se indica también que el contrato con la entidad Certificadora es el 2019-1777 Gestión de Seguridad Electrónica SA, cuyo objeto es "*Prestar el servicio de certificado de firma digital de personas, certificado de servidor seguro, certificado de persona jurídica entidad empresa, servicio de estampado cronológico de documentos con salida en formato PDF/A nativo, así como el servicio de soporte técnico de los anteriores elementos en los sistemas de información de la Secretaría Distrital de Movilidad",* en el cual se establece una capacidad para 42 firmas con una vigencia de 12 meses.

Las firmas o certificados digitales tienen como propósito que las firmas digitales se utilicen para autenticar información digital; en la Entidad la requieren para documentos como expedientes para las autoridades de tránsito (comunicaciones masivas); ésta reemplaza la firma física en grandes volúmenes de documentos digitales. Cuando se trata de firmas de las órdenes de pago para los contratistas aplica para los ordenadores del gasto (interacción entre entidades – SHD Movilidad), en los procesos automatizados y digitalizados.

Se aporta como evidencia el listado de firmas GSE de fecha 25/05/2020, con una relación de 32 funcionarios inscritos en la misma; en donde se observa que se duplican nombres de suscriptores con la misma fecha de envío al cliente y no se hace referencia a la situación que genera esta duplicidad en la columna de observaciones

Por último, se realizan las siguientes precisiones por parte de la OTIC:

- El correcto uso corresponde a cada persona, se controla a través del ente certificador.
- Todos los documentos firmados de forma digital deben firmarse en físico una vez termine la situación de calamidad (autenticidad de documentos).
- El control de OTIC corresponde a establecer el protocolo para su utilización (Circular 05 y 06 de 2020).
- En el protocolo de la firma mecánica solo en dos casos puntuales no se pudo certificar por inconvenientes técnicos, los cuales fueron plenamente identificados.
- Se están publicando documentos sin firma en SIMUR (estudios para la movilidad); en este caso se debe verificar con cada dependencia que publica. Ellos determinan su validez. Un estudio de tránsito viene de un ente privado, el cual la SDM aprueba a través de un documento, pero es cada área o dependencia quien valida el protocolo para la publicación de la información.

De igual manera y teniendo en cuenta lo establecido con el Decreto 1078 de 2015, el Manual de Gobierno Digital y la Guía 10 para la preparación de las TIC para la continuidad del negocio, se atendió la siguiente solicitud expuesta en el mismo documento:

a) En el año 2018, la OCI le recomendó a la OTIC, "*Dar continuidad al proceso de implementación del DRP (Plan de Recuperación ante Desastres) e Incluir dentro de los proyectos de implementación del DRP las demás sedes de la entidad.*" En tal sentido, sírvanse informar el estado de avance del plan en mención (DRP).

Respuesta OTIC:

Se definieron las actividades que se realizarán en la Gestión de continuidad, para los recursos tecnológicos administrados por el Operador tecnológico en la entidad, para lo cual se adjuntan los documentos PLAN DE CONTINUIDAD y GESTION DE CONTINUIDAD.

Verificación de la OCI:

De acuerdo a la evidencia aportada se observa que la entidad a través del documento GESTIÓN DE CONTINUIDAD de fecha marzo 2020, identifica:

- Actividades PHVA Gestión de Continuidad.
- Procedimiento de la gestión.
- Diagrama de actividades.
- Roles y responsabilidades.
- Entradas y salidas del proceso.
- Indicador de efectividad de las pruebas PRT.

En el desarrollo de la mesa de trabajo con la OTIC se realizan las siguientes aclaraciones al equipo auditor:

- DRP protege contra desastres exteriores y es costoso tener replica de una plataforma TI fuera de casa; en ocasiones más costoso que la misma infraestructura con la que se cuenta al interior de la entidad.
- Se está adelantando la implementación de la renovación tecnológica, se migro el Datacenter al primer piso. En este momento se tiene alta seguridad y disponibilidad en conectividad y almacenamiento y se está trabajando migración data en la nube.
- Se está trabajando en la renovación, actualización TI y automatización de lo que se tiene, para definir la línea base TI.
- La OTIC cuenta con un presupuesto asignado que le permite atender las necesidades prioritarias, no cuenta con recursos para ejecutar este tipo de proyectos (DRP).
- La continuidad depende de la articulación transversal, por ejemplo, la atención de los ciudadanos en ventanilla puede darse de diferentes maneras sin que sea específicamente a través de TIC.

- Se tiene como avance, lo relacionado con el Plan de continuidad del negocio – BCP, para lo cual se ha implementado alta disponibilidad, en componentes como:
  - Eléctrico.
  - Aire acondicionado.
  - Almacenamiento.
  - Conectividad Core.
  - FireWall seguridad perimetral.
  - Canales de Internet.
  - Nube.
- Tener un plan de continuidad se convierte en un tema preventivo.
- La parte operativa está cubierta con las políticas de backup y los medios se tiene externamente, almacenados, custodiados y preservados (Banco Popular - Alpopular).

En la actualidad, luego del proceso de renovación tecnológica, traslado del Datacenter, implementación de alta disponibilidad, se tiene el plan de continuidad y la siguiente fase DRP se tiene proyectada para implementar en el siguiente cuatrienio, con la participación de la Alta Dirección y en articulación transversal, con las diferentes dependencias de la Entidad, y dentro de un enfoque de mejoramiento continuo.

Si bien se aportan los documentos evaluados como parte del avance de la gestión; no se evidencia de manera clara cuál fue la participación de la alta dirección en la construcción de los documentos (PLAN DE CONTINUIDAD y GESTION DE CONTINUIDAD) y cómo se aprobó en el marco del Comité de Gestión y Desempeño, de acuerdo con lo definido en el Artículo 6 de la Resolución 256 de 2018 y cómo se socializó e implementó. Lo anterior aunado a que tal como se manifestó en el desarrollo de la mesa de trabajo, el Plan de Recuperación ante Desastres no corresponde sólo a una gestión tecnológica, sino que corresponde a un tema trasversal a nivel institucional.

De igual manera se identifica a través del documento PLAN DE CONTINUIDAD de fecha 15/03/2020, cuyo objetivo principal es "*Tomar medidas que permitan el óptimo funcionamiento de la plataforma tecnológica en la secretaria de Movilidad ante la pandemia por el Coronavirus (COVID-19)*."; las principales acciones implementadas por la entidad con relación a:

- TIC- Infraestructura Tecnológica en alta disponibilidad.
- TIC - Infraestructura Tecnológica.
- TIC - Infraestructura Tecnológica y Recurso Humano.
- Medios TIC habilitados.

b) Así mismo, y dada la contingencia COVID-19, es importante conocer el plan de contingencia documentado que desde la alta dirección se estableció la SDM para afrontar el cumplimiento de su misionalidad.

Respuesta OTIC:

En el documento Plan de contingencia adjunto se definen los procedimientos a seguir, los recursos a utilizar y los controles definidos para atender la prestación de los servicios ante la contingencia Covid-19.

Verificación de la OCI:

La evidencia aportada corresponde al documento PLAN DE CONTINUIDAD FRENTE AL CORONAVIRUS (COVID 19); que, si bien en su Tabla de Contenido identifica aspectos como los relacionados a continuación, los mismos no se desarrollan en el documento mencionado:

- Marco para la preparación de las TIC para la continuidad tecnológica Frente al coronavirus (covid-19).
- Descripción detallada de la preparación de las TIC para la continuidad de la SDM ante el coronavirus (covid-9).
- Requerimientos de tiempos de recuperación ante las afectaciones por Coronavirus (covid-19)
- Análisis de impacto tecnológico en SDM ante coronavirus (covid-19).
- Identificación de funciones y procesos.
- Evaluación de impactos operacionales.
- Identificación de procesos críticos.
- Establecimiento de tiempos de recuperación.
- Identificación de recursos.
- Identificación de procesos alternos.
- Gestión del riesgo ante el coronavirus (covid-19).
- Acciones implementadas especialistas.
- Medios habilitados.

Si bien la estructura definida en la Tabla de Contenido del documento aportado como evidencia, presenta de manera general los aspectos referenciados en la Guía 10 para la preparación de las TIC para la continuidad del negocio de MINTIC; estos no se desarrollan en el documento aportado.

En la mesa de trabajo se precisa por parte del equipo de la OTIC que los documentos PLAN DE CONTINUIDAD y GESTIÒN DE CONTINUIDAD, fueron documentos socializados al interior de la OTIC y no institucionalmente. Se hace referencia a la gestión de tecnología y servicios tecnológicos, el primer paso fue fortalecer la gestión tecnológica, políticas, protocolos y data; con lo cual se tiene la base para trabajar la parte trasversal y operativa.

c) Si bien la SDM creó un instructivo proceso "*Teletrabajo Versión 1.0*", para cumplir con la normatividad vigente y garantizar el aislamiento preventivo obligatorio a través del concepto de "*Trabajo en casa*"; se solicita se informe la cantidad de funcionarios y contratistas que están haciendo uso de la VPN u otra alternativa como solución de conectividad, a corte del recibo de esta comunicación

Respuesta OTIC:

A corte 22 de mayo de 2020 en total 1162 usuarios se conectan utilizando la conexión VPN C2S, de los cuales, 1145 usuarios se conectan utilizando credenciales de dominio (funcionarios y contratistas) y 17 usuarios con credenciales locales de FW (proveedores). Se adjunta documento ConexionesVPN con la cantidad de conexiones VPN y archivo UsuariosVPN con los funcionarios y proveedores que hacen uso de la VPN

Verificación de la OCI:

Conforme a la evidencia aportada se observa:

Usuario
pbmuser1
belltech
usersdh
siconvpn
softmanagement
dextera
usersecgeneral
gr_software_management
supercadeamericas1
supercadeamericas2
supercadeamericas3
supercadeamericas4
supercadeamericas5
supercadebosa1
redcomputo1
redcomputo2
redcomputo3

Conforme la anterior información se solicita a la OTIC, en el desarrollo de la mesa de trabajo, indicar cuál es el control que se realiza sobre las conexiones VPN de proveedores, a que información tienen acceso y cuales políticas de seguridad se están aplicando.

Sobre este particular la OTIC indica que todas cumplen con certificado de seguridad punta a punta, desde los dos puntos donde se tiene la conexión. Cada uno tiene un propósito específico, todas tienen políticas de seguridad externa y políticas específicas punta a punta y todas se encuentran debidamente identificadas. Adicionalmente se indica que se tiene un plan de revisión periódica y seguimiento de VPN.

d) Reporte de funcionarios o contratistas que no hayan podido trabajar vía VPN y para este caso que solución de conectividad previó la SDM.

Respuesta OTIC:

La solución para aquellos funcionarios que no solicitaron creación de VPN es la suite GOOGLE APPS la cual es un conjunto de aplicaciones que nos permite organizar de forma sencilla todo el trabajo; y la comunicación entre los distintos funcionarios de la entidad con diversas herramientas para la gestión del correo electrónico, mensajería instantánea, planificación de reuniones y tareas, generación de documentos y hojas de cálculo.

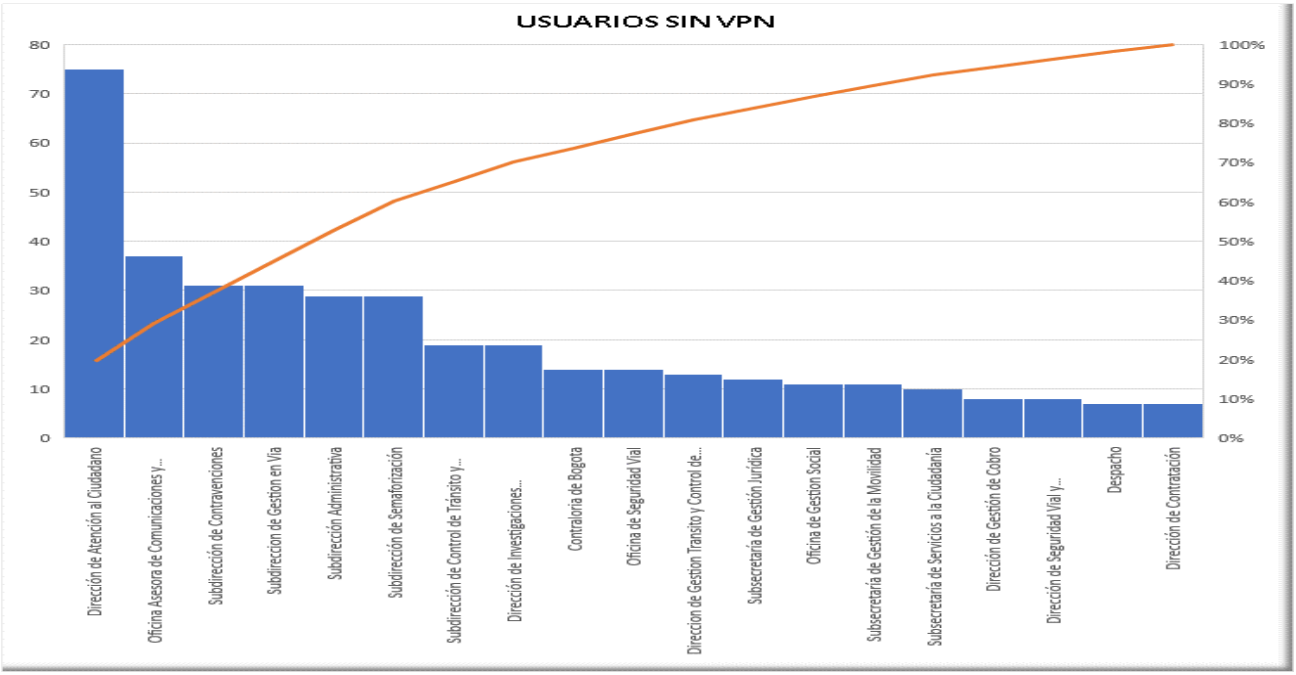
Verificación de la OCI:

La evidencia aportada (documento llamado GOOGLE APPS – ACCESO A INFORMACIÓN DE LA SDM) corresponde a la descripción de las funcionalidades de la herramienta.

Respecto a cómo se garantiza el control sobre la información que se está generando a través de google apps, la OTIC en el desarrollo de la mesa de trabajo, realiza las siguientes aclaraciones:

- Cada carpeta compartida tiene acceso definido por el jefe de dependencia. Acceso total o acceso lectura.
- Así mismo, la plataforma de correo y colaboración cuenta con Vault con el que la Entidad puede conservar, bloquear, buscar y exportar datos para responder a las necesidades de conservación, control y auditoria.

De acuerdo a la evidencia aportada por la OTIC (Listado de usuarios SIN VPN.xlsx), se observa que 474 servidores de la entidad no se encuentran trabajando con VPN; de los cuales la mayor parte corresponden a la Dirección de Atención al Ciudadano y la Oficina Asesora de Comunicaciones, conforme se muestra a continuación:



Fuente: Listado de usuarios SIN VPN.xlsx

e) Listado de equipos de cómputo por dependencia (*portátiles, PC escritorio, Impresoras, Escáner*), que, con el fin de atender la contingencia a través de teletrabajo o trabajo en casa, han salido de la Secretaria y los controles establecidos para garantizar su adecuada custodia

Respuesta OTIC:

La dependencia encargada de autorizar la salida de equipos de cómputo es la Subdirección Administrativa, se adjuntan los documentos enviados por ellos llamado Ordenes de salida y SALIDA DE ELEMENTOS con la relación de elementos autorizados.

Verificación de la OCI:

La evidencia aportada da cuenta del retiro de varios equipos por parte de un funcionario de la entidad, con destino a la calle 13 (OTIC) en fechas 30/03/2020 (2) y 1 con varios elementos el día 13/05/2020, sin que se evidencie en este último bajo quien recae la responsabilidad de su custodia o el área al que van a ser asignado estos elementos.

Respecto a cuáles son los controles que desde la OTIC se han implementado para validar el estado con el que se entregan los elementos y su posterior recibo una vez termine la cuarentena, se indica en la mesa de trabajo:

- Se tiene una ficha por cada máquina, para los movimientos de las maquinas entre sedes hay una ficha que indica el estado visual de la misma.
- Como este caso es diferente (Covid 19) a lo que normal se tiene, cuando se haga el retorno se validará con Subdirección Administrativa para hacer la revisión correspondiente

Con relación al protocolo para controlar el ingreso de los equipos a la entidad, la OTIC indica que se va a proponer la participación de esta oficina en el protocolo de ingreso a que adopte la Subdirección Administrativa

Por último y sobre la pregunta de qué controles se establecieron para validar que equipos, que estaban en poder de los funcionarios en la entidad, fueron retirados de la misma para trabajar desde casa; indica la OTIC que en la mayoría de los casos está controlada por que se informaron (todos los equipos que pasaron por el operador para la instalación de VPN están controlados). Se indica de igual manera que en teoría están relacionados en las minutas de vigilancia de la entidad.

f) Informar si dada la contingencia y la conectividad con VPN, la entidad ha evaluado e identificado nuevos riesgos que se han hecho visibles durante la contingencia. Adjuntar matriz de tratamiento.

Respuesta OTIC:

Se adjunta documento llamado RIESGOS TECNOLÓGICOS POR EL COVID 19, con la identificación y evaluación de nuevos riesgos.

Verificación de la OCI:

En el documento se identifican entre otros, los siguientes riesgos:

- Arquitectura de red general: “los empleados pueden no ser los únicos usuarios de estas VPN; los hackers también pueden usar su VPN, sobre todo a través de los equipos finales utilizados, este es otro de los factores de riesgo”.

- Endpoints: en implementaciones rápidas como las que estamos viendo actualmente, los puntos finales de los trabajadores que lo hacen a distancia pueden tener que usar cualquier computadora que tengan en casa. Estas pueden ser máquinas antiguas con poca potencia y sin parches. Actualmente en la SDM tenemos una visibilidad limitada de su configuración y ninguna garantía sobre su seguridad. Es posible que estas computadoras ya estén infectadas con malware, que puede aprovechar la oportunidad de conexión a una VPN para infectar otras máquinas, incluidos los sistemas críticos dentro de la empresa. Si el punto final es parte de una botnet o tiene un troyano de acceso remoto instalado, los atacantes pueden usar el punto final como un pivote en la red corporativa.

- Control de acceso: Inicialmente la habilitación de contraseñas con complejidad sería de gran ayuda. Esta es una configuración que se encuentra en las políticas de la entidad, sin embargo, según nos comentan los integrantes antiguos del grupo, no se ha podido

implementar por problemas asociados a la resistencia al cambio. Por otro lado, la autenticación multifactor con elementos como certificados de cliente o tokens de hardware o al menos SMS serían de gran ayuda en el fortalecimiento de la seguridad en la conexión y permitiría otorgar más accesos, pero implicaría costos.

- Chats y redes sociales: Una vez conectados a la VPN los usuarios acceden a la red utilizando los recursos de la SDM, es decir, la navegación se da a través de esta conexión, por lo que el uso doméstico aumenta las conexiones con aplicaciones que no son propiamente laborales. Kuaishou (tiktok), youtube, whatsappweb, RTCP (multimedia), icecast straeaming de audio, Skype

- Conexiones VPN fuera del horario laboral: conexiones que generan en horarios fuera de la jornada laboral y que no son normales de cara a la operación (00:00 y 04:00).

Si bien se han identificado los riesgos se recomienda dar prioridad a la definición de controles, valoración y tratamiento de los riesgos conforme lo establece la ISO 31000 y la guía de Riesgos del DAFP.

g) Informe de monitoreo y seguimiento del mapa de riesgos de seguridad digital, con corte a abril 30 de 2020.

Respuesta OTIC:

Se adjunta documento llamado INFORME MONITOREO DE SEGURIDAD POR COVID 19, con el monitoreo y seguimiento del mapa de riesgos de seguridad.

Verificación de la OCI:

Resultado de la mesa de trabajo realizada con la OTIC, se aporta evidencia adicional, la cual corresponde a:

- Informe de Monitoreo y Seguimiento Mapa de Riesgos: En el documento se presenta el resultado del seguimiento realizado con corte abril 30 de 2020 a los controles establecidos en el mapa de riesgos institucional correspondiente al Evento Potencial: Implementación de la Política de Seguridad Digital deficiente e ineficaz para las características y condiciones de la Entidad.
- Informe Gestión de Riesgos corte 30 de abril: La evidencia corresponde a la gestión realizada desde la OTIC respecto a los riesgos de seguridad de la información, llevada a cabo a través de la ejecución del contrato No. 2019-1813 cuyo monitoreo y control se realiza a través de la herramienta Global Suite, y que identifica los siguientes elementos:
    - Firewall
    - Gestión de Continuidad Tecnológica
    - Gestión de Servidores
    - Sophos Central On-Cloud

- Todas las Aplicaciones
- Gestión Licenciamiento de Software
- Gestión Seguridad Informática

Esta nueva evidencia también incluye la vinculación de los riesgos identificados a raíz del COVID 19 con la norma técnica ISO/IEC 27001:2013, así:

- A.9.4.1. Restricción de acceso a información
- A.9.4.2. Procedimiento de ingreso seguro
- A.9.4.4. Uso de programas utilitarios
- A.11.2.9. Escritorio seguro y pantalla limpia
- A.12.2.1. Controles contra código malicioso
- A.12.6.2. Instalación de software utilizado por usuarios en la red
- A.17. Continuidad en la seguridad de la información.

Por último, se observa en este mismo documento el avance del Plan de tratamiento de los riesgos COVID 19:

Plan de tratamiento	Estado actividades	Avance	Estado Control
Eliminación de publicaciones inseguras		33%	EN PROCESO
Identificar publicaciones realizadas desde segmentos de red diferentes a la DMZ	Implementada		
Eliminar servicios inseguros expuestos	No Implementada		
Configurar publicaciones desde la DMZ	No Implementada		
Configuración de acceso BP		33%	EN PROCESO
Documentación Best Practice	Implementada		
Configuración Sophos	No Implementada		
Configuración Palo Alto	No Implementada		
Crear y documentar procedimiento de uso de software		0%	EN PROCESO
Sesión de entendimiento	No Implementada		
Documentar procedimiento	No Implementada		
Implementación	No Implementada		
Documentación de requerimientos mínimos de seguridad		100%	COMPLETADO
Prerrequisitos de información	Implementada		
Documentación	Implementada		
Ajustes a la documentación	Implementada		
Procedimiento de respaldos		100%	COMPLETADO
Ajustar procedimiento de respaldos existente	Implementada		
Proceso de entregas y despliegue		100%	COMPLETADO
Ajustar documentación existente	Implementada		
Implementación de firma digital de documentos		83%	EN PROCESO
Implementación	Implementada		
Metadata CleanUp AD	Implementada		
Afinamiento procedimiento	Parcialmente Implementada		
Hardening		83%	EN PROCESO
Crear plantilla de hardening Windows	Implementada		
Crear plantilla de hardening Linux	Implementada		
Implementación de hardening	Parcialmente Implementada		
Instalación de antivirus en servidores		83%	EN PROCESO
Levantamiento de información	Implementada		
Documentación de excepciones	Implementada		
Instalación de software de antivirus en servidores	Parcialmente Implementada		

Plan de tratamiento	Estado actividades	Avance	Estado Control
Política de seguridad y privacidad de la información		67%	EN PROCESO
Actualización Política 2016	Implementada		
Recreación de política	Implementada		
Publicación y oficialización	No Implementada		
Políticas especificas de seguridad de la información		33%	EN PROCESO
Actualizar políticas especificas de seguridad	Parcialmente Implementada		
Aprobación Planeación	Parcialmente Implementada		
Publicación y oficialización			
Configurar monitoreo		67%	EN PROCESO
Configurar logs Imperva	No Implementada		
Configurar logs Sophos	Implementada		
Configurar logs Proxys	Implementada		
Configurar servidor IPA		100%	COMPLETADO
Implementación plataforma IPA	Implementada		
Instalación de agentes	Implementada		
Presentación de Propuesta	Implementada		
Configurar certificados digitales en servicios internos y externos		83%	EN PROCESO
Template de certificado WEB	Implementada		
Portal solicitudes	Implementada		
Implementación	Parcialmente Implementada		
Gestión de vulnerabilidades técnicas		50%	EN PROCESO
Gestión de vulnerabilidades	Parcialmente Implementada		
Crear metodología de gestión de activos de información(Clasificación, valoración, calificación, etiquetado)		100%	COMPLETADO
Crear metodología y documentar	Implementada		
Realizar el levantamiento de activos de información		50%	EN PROCESO
Levantamiento de activos	Parcialmente Implementada		
Configuración Controles Gsuite		40%	EN PROCESO
Documentar estado actual y propuestas de mejora	Implementada		
Escalamiento Xertica	Parcialmente Implementada		
Implementación de controles Xertica	No Implementada		
Implementación de controles Selcomp	No Implementada		
Disclaimer	Parcialmente Implementada		

Plan de tratamiento	Estado actividades	Avance	Estado Control
Implementar contraseña segura		0%	EN PROCESO
Aprobación de políticas	No Implementada		
Implementación	No Implementada		
Bloqueo de pantalla		0%	EN PROCESO
Aprobación de políticas	No Implementada		
Implementación	No Implementada		
Optimización de configuraciones en el Firewall		25%	EN PROCESO
Depuración reglas ANY	No Implementada		
Limitar reglas de navegación	Implementada		
Depurar reglas de NAT	Parcialmente Implementada		
Estandarización de configuraciones	No Implementada		
Configuración aplicaciones	No Implementada		
Documentación de reglas limitadas	No Implementada		
Bloqueo de dispositivos externos de almacenamiento.		0%	EN PROCESO
Diseñar e implementar controles	No Implementada		
Documentar proceso	No Implementada		

Fuente: Informe Gestión de Riesgos corte 30 de abril

h) Resumen de las posibles violaciones de seguridad que se hayan presentado durante el periodo enero abril del 2020 comparado con el mismo periodo del año 2019, el análisis realizado al resultado obtenido y las estrategias implementadas adoptadas por la entidad para controlar las situaciones presentadas.

Respuesta OTIC:

Se adjunta documento denominado INFORME VIOLACIONES DE SEGURIDAD, con las posibles violaciones de seguridad, el análisis realizado, el resultado obtenido y las estrategias implementadas adoptadas por la entidad para controlar las situaciones presentadas

Verificación de la OCI:

De conformidad con la evidencia aportada, las posibles violaciones de seguridad corresponden a las siguientes situaciones:

1. Phishing: Se evidenció recepción de correos electrónicos con dominio @minsalud.gov.co, ante esto se realizó seguimiento general y la plataforma de correo con los controles actuales aplicó filtros antispam que mostraron advertencias y envío a la carpeta de correo no deseado en todos los casos. Frente a esto de todos modos se está trabajando para implementar controles adicionales y cambiar las acciones antispam para que sean más restrictivas.

2. ZOOM: En esta cuarentena, se evidenció el uso de ZOOM como plataforma para realizar las sesiones trabajo corporativo. La plataforma tiene vulnerabilidades críticas que el mismo fabricante tuvo que publicar. Ante esto inicialmente el software de protección endpoint de sophos bloqueó el uso de la herramienta, sin embargo, la OTIC ordenó eliminar el bloqueo y emitir comunicados para incentivar el uso de las herramientas corporativas con las que cuenta la entidad.

3. Conexiones anómalas de servidores de datatools a direcciones IP reportadas como BOT maliciosas: Ante esto se quitaron los permisos de salida a internet de los servidores de datatools y se escaló al proveedor, quién indicó que el equipo identificado se trataba de un pivote utilizado por los especialistas para conexión remota. Para este caso puntual, se realizó un escaneo externo al pool de direcciones IP públicas de la entidad, se identificaron servicios inseguros publicados y se ejecutó cambio (491) para mitigar a través del cierre y limitación de las publicaciones. Se encuentra en curso un plan de trabajo que pretende eliminar las publicaciones que se realizaron en el pasado, directamente desde las subredes de servidores ya que todas las publicaciones deben estar desde la red DMZ.

4. Entendiendo que la conexión VPN es una extensión de la red LAN de la SDM, se evidenciaron sesiones de los funcionarios que desde la conexión VPN se conectan a redes sociales, portales de streaming y demás navegación no laboral. Se elaboró un comunicado que será emitido en los próximos días para informar la limitación de dicha navegación.

5. Conexiones remotas haciendo uso de software libre o software de prueba (TeamViewer – AnyDesk): La entidad no cuenta con un software licenciado para realizar labores de soporte remoto, así que AnyDesk se utiliza por los analistas de soporte, en ese sentido se están validando alternativas de limitar el uso de estas herramientas solo para este fin.

Se informa de manera adicional que se llevó a cabo la restricción al acceso a aplicaciones como TIC TOC a todos los usuarios de la entidad.

i) Listado de aplicaciones autorizadas para acceder de forma remota a través de la VPN, identificando el correspondiente licenciamiento.

Respuesta OTIC:

Se adjunta documento llamado APLICACIONES Y SERVICIOS VPN, con las funciones y aplicaciones importantes para la operatividad de la Secretaria de Movilidad, que se pueden acceder desde cualquier conexión VPN.

Verificación de la OCI:

La evidencia aportada no indica si las aplicaciones relacionadas, a las cuales se puede acceder remotamente a través de VPN se encuentran licenciadas.

j) Análisis de afectaciones de los ANS de aquellas aplicaciones catalogadas como críticas y que tiene relación directa con los ciudadanos con usuarios internos.

Respuesta OTIC:

Se adjunta documento llamado INFORME ANÁLISIS AFECTACIONES ANS APLICATIVOS, con las aplicaciones que presentaron afectaciones de ANS

Verificación de la OCI:

La evidencia aportada corresponde a:

Aplicación	Servidor	Disponibilidad	Observaciones
ARCGIS	GISPSM05	100%	N/A
BI	SIMUR_BIS	100%	N/A
BIBLIOTECA DIGITAL	SIMUR_IN_DBI	100%	N/A
BICIWEB	BICIWEB	100%	N/A
CENSOBICI	CENSO_BICITAXI	100%	N/A
CONTROL ACCESO	WEBFSM01	100%	N/A
DUUPS	WEBFSM01	100%	N/A
EXCEPCIONES	SIMUR_HTTP	100%	N/A
FACTORCALIDAD	WEBFSM01	100%	N/A
INTRANET	INTRANET_2017	100%	N/A
LASERFICHE	MOVBOG006	100%	N/A
MOODLE	MOODLE_INTRA	100%	N/A
PORTAL MOVILIDAD (SDM)	PORTALWEB_APP	100%	N/A
PORTAL SIMUR	SIMUR_PORTAL_PROXY	100%	N/A
PQRWEB	WEBFSM01	100%	N/A
RED EMPRESARIAL	DRUPAL	100%	N/A
RUTAPILA	WEBFSM01	100%	N/A
SICAPITAL	SICAPITALWLDESA	100%	N/A
SIGAT	SIGAT	100%	N/A
SIGI	SIMUR_IN_DBI	100%	N/A
SIGRUP	SIGRUP	100%	N/A
SIMUR	SIMUR_SOA	100%	N/A
SIPAC	SDMPRDSIC04_SIPAC	100%	N/A
SIRC	WEBFSM02	100%	N/A
TABLEAU	APP_TABLEU	100%	N/A
VIDEOS	WEBFSM01	100%	N/A

Fuente: INFORME ANÁLISIS AFECTACIONES ANS APLICATIVOS.

El mismo documento indica que: “no existe afectación a los ANS, todas las aplicaciones funcionaron durante la cuarentena obligatoria”.

ANALISIS DE RIESGOS DESDE LA PERSPECTIVA DE LA OCI.

Si bien la OTIC ha tomado medidas para permitir la operación de la SDM en esta contingencia, el hecho de no contar con un plan de continuidad de negocio y su DRP, podrían ante cualquier otro evento limitar la capacidad de respuesta de la Secretaria, no solo desde la óptica tecnológica, sino desde la perspectiva de la operación normal, en temas como por ejemplo Semaforización, SICON (Contravenciones), Excepciones, SAE, PERNO, SAI y LIMAY entre otros.

De forma adicional, dada las vulnerabilidades que representa para los equipos de la SDM el estar conectado a través de VPN, es importante que se tomen los controles necesarios que permitan identificar de forma oportuna la materialización de eventos que puedan afectar los servicios de la Secretaria desde el punto de vista de la Disponibilidad, Confidencialidad e Integridad de la información.

CONCLUSIONES Y RECOMENDACIONES:

Si bien se destacan fortalezas como la experticia del equipo de la OTIC que atendió el seguimiento realizado en los diferentes aspectos que fueron objeto de evaluación, así como la entrega oportuna de los soportes o evidencias que fueron solicitadas por la OCI en el desarrollo del mismo; es importante indicar que en el desarrollo del seguimiento se evidenciaron las siguientes oportunidades de mejora:

- Teniendo en cuenta que en la relación suministrada como evidencia del listado de las firmas GSE de fecha 25/05/2020, se evidenciaron situaciones como la duplicación de nombres con la misma fecha de envío al cliente (dos casos), algunos de los nombres relacionados ya no se encuentran en los cargos en los cuales estaban vinculados en la fecha de envío del certificado (1 caso), y funcionarios relacionados que ya no están en la entidad (1 caso); se recomienda validar esta información y revisar la capacidad real actual de firmas, así como el cumplimiento de la obligación estipulada en el contrato 2019-1777 relacionada con:

  Clausula cuarta: Numeral 15: “… reemplazo de certificados digitales si hay lugar a ellos, renovaciones si hay lugar a ello, etc”

  Respecto al documento preliminar socializado a través de correo electrónico de fecha 03/07/2020 a la Oficina de Tecnologías de la Información y Comunicaciones (OTIC); a través de correo electrónico del 08/07/2020 la OTIC indica con referencia a los duplicados que los usuarios señalados dejaron vencer las descargas de los certificados y se tenía que volver a solicitar y que ya se efectuó el requerimiento a GSE para ajustar esa novedad. Referente a la relación de funcionarios que ya no se encuentran laborando en la entidad, antes de su retiro tenía que firmar cuentas como ordenadora del gasto y su certificado se vencía en diciembre de 2019 por lo que se tuvo que renovar, se precisa que ese cupo ya fue cancelado.

Validación de la OCI:

Lo justificado corresponde a correcciones sobre lo observado por el equipo auditor en el desarrollo del seguimiento, que si bien subsana lo evidenciado no garantiza que la situación presentada no vuelva a materializarse por lo cual se mantiene la recomendación dada en el documento preliminar.

- Implementar los controles que permitan garantizar que se esté dando cumplimiento por parte de los jefes de dependencias a los lineamientos establecidos por la OTIC respecto a las dos formas de firma digital ante la situación actual de emergencia sanitaria y económica; lo anterior en razón a que en el ejercicio trasversal realizado por la OCI en el desarrollo de los diferentes seguimientos que adelanta en estos meses de emergencia, se observó que los documentos SDM-SF-86477 de 2020 de fecha 10/06/2020, SDM-SA-86479-2020 del 16/06/2020 y SDM-OTIC-82147-2020 del 29/05/2020 no aplica los protocolos de la entidad para la gestión de las firmas indicadas en el presente seguimiento (Utilización de la firma mecánica para la suscripción de los documentos a cargo de los directivos de la SDM).

  A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

  > *"La Entidad definió la entrega de firmas digitales mecánica a cada uno de los jefes de la entidad, para aquellos jefes que no poseían firma digital; la OTIC a través del operador tecnológico SELCOMP implemento una firma digital mecánica como una solución tecnológica que ofrece tanto seguridad como confianza a los documentos electrónicos emitidos. Esta solución se implementó y socializo personalmente a cada uno de los jefes a quienes se les asigno y se les indico la importancia del medio, los niveles de confianza de la firma digital mecánica, frente no tenerla mediante este mecanismo; así como los criterios y recomendaciones de seguridad."*

  Validación de la OCI:

  Lo justificado no garantiza que la situación presentada vuelva a materializarse por lo cual se mantiene la recomendación dada en el documento preliminar

- En virtud del alto volumen de información que se maneja en la SDM y la repercusión económica y legal que genera un gran impacto sobre la vulnerabilidad de la misma; se hace necesario establecer mayores controles con el fin de garantizar su adecuado manejo, en términos de Disponibilidad, Confidencialidad e Integridad. Dado lo anterior, la OCI reitera su recomendación de dar continuidad a la implementación del PRD de tal manera que la entidad garantice la restauración oportuna de las operaciones esenciales en cualquier tipo de evento disruptivo

  A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

  > *"Estos se garantizan mediante el subsistema de seguridad de la información implementado en la Entidad que involucra la información, hardware, software, usuarios, políticas y protocolos*

establecidos para producir, recolectar, almacenar, proteger, disponer y custodiar, como el activo más importante de la Entidad, su información".

Validación de la OCI:

Lo justificado, si bien hace parte de la gestión adelantada por la entidad y que fue observada también en el desarrollo del seguimiento, está sujeta a oportunidades de mejora que fueron objeto de recomendación tanto en el presente documento con en el seguimiento realizado por la OCI a la implementación de MSPI realizado en la vigencia 2018, conforme lo anterior se mantiene la recomendación dada en el documento preliminar

- En cumplimiento de lo dispuesto en la Resolución 256 de 2018 Artículo 6 (Comité de Gestión y Desempeño), se recomienda a la OTIC documentar la participación de la alta dirección en la aprobación de los documentos que hacen parte del avance de la gestión adelantada respecto al Plan de Continuidad de la entidad y el Plan de Recuperación ante Desastres (PRD).

  A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

  "La OTIC como líder para el Plan de Recuperación ante Desastres DRP, siempre ha tenido la iniciativa en las actividades del DRP en la Secretaria de Movilidad; por tal razón inicia con el plan de renovación tecnológica en diferentes fases de acuerdo a los recursos asignados por la Alta Dirección que considero importante el proceso ante la obsolescencia tecnológica y la baja madurez TI de la Entidad en su momento; durante este proceso, se ha trabajado en BCP que protege contra problemas de hardware, desarrollando actividades como cambio de servidores, dotación de un datacenter, cambio de todos los elementos de conectividad de la entidad, migración a IPv6, implantación de lata disponibilidad de en seguridad, conectividad, almacenamiento, entre otros. Así mismo, la infraestructura tecnológica se mantiene monitoreada y gestionada a cargo del operador tecnológico y los líderes funcionales de cada aplicación tienen la responsabilidad de documentar e implementar alternativas para el óptimo funcionamiento de las aplicaciones CORE de la entidad ante un disrupto. Así el DRP que protege contra desastres exteriores inicialmente implementado por la OTIC abarca actividades a lo largo de toda la entidad con los recursos disponibles hasta el momento, que requieren la participación activa y la cooperación de distintas dependencias. Razón por la cual la alta dirección siempre está enterada de las actividades y procesos ejecutados"

  Validación de la OCI:

  Lo justificado no garantiza la subsanación de la situación observada en el desarrollo del seguimiento, por lo cual se mantiene la recomendación dada en el documento preliminar

- Se recomienda socializar a nivel institucional los diferentes documentos que se han implementado en la OTIC relacionados tanto con el Plan de Continuidad como al Plan de Continuidad frente al Coronavirus (COVID 19).

A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

> *"En reuniones conjuntas entre el la OTIC y el operador tecnológico SELCOMP se generaron documentos de plan de continuidad ante COVID-19, manuales con protocolos de Bioseguridad y Plan para trabajo en casa ante COVID -19; así como se publicaron los canales de acceso a la mesa de servicio por parte de los funcionarios, los protocolos y formatos para VPN, disposición y traslado de recursos TI, entre otros"*

Validación de la OCI:

Lo justificado no garantiza la subsanación de la situación observada en el desarrollo del seguimiento por lo cual se mantiene la recomendación dada en el documento preliminar

- Se recomienda desarrollar el documento PLAN DE CONTINUIDAD FRENTE AL CORONAVIRUS (COVID-19) conforme la estructura definida en la Tabla de Contenido del documento aportado como evidencia, y de acuerdo a las guías que sobre el particular a emitido el Mintic (Eliminado).

  A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

  > *"El Plan de Continuidad Frente al Coronavirus, se construye a partir de los lineamientos definidos por la Entidad, liderados por la OTIC para el componente TI y articulados en conjunto con el operador tecnológico; el cual fue entregado y cumple con los requisitos necesarios de acuerdo atender la contingencia; así mismo, será integrado al Plan de Continuidad Institucional, cumpliendo con los requisitos del MinTIC."*

  Validación de la OCI:

  Se aporta nueva evidencia correspondiente al documento PLAN DE ACCIÓN PARA CONTINUIDAD TECNOLÓGICA FRENTE AL CORANOVIRUS (COVID-19) en el cual se atendió la recomendación dada en el informe preliminar respeto a desarrollar el documento de acuerdo a como se definía en su tabla de contenido; por lo anteriormente expuesto se valida como una Corrección en el desarrollo del ejercicio de seguimiento y se retira la recomendación realizada en el documento preliminar.

- Teniendo en cuenta las debilidades observadas en el control de los equipos que han sido retirados de la entidad para realizar trabajo en casa, descritos en el acápite DESARROLLO DEL INFORME; se recomienda fortalecer los controles relacionados con la ubicación actual real de los equipos retirados en la entidad e implementar las acciones o protocolos que se consideren pertinente para garantizar que los equipos que se reintegren a la entidad se encuentren en condiciones adecuadas para su uso.

  Respecto al documento preliminar socializado a través de correo electrónico de fecha 03/07/2020 a la Oficina de Tecnologías de la Información y Comunicaciones (OTIC); a través

de correo electrónico del 08/07/2020 la OTIC aporta el protocolo que se ha trabajado con la Subdirección Administrativa sobre este aspecto.

De igual manera y a través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

> *"La OTIC por intermedio de la mesa de servicio tiene control de los equipos entregados a cada uno de los funcionarios de la entidad ante el COVID-19 y son registrados en la herramienta de gestión ARANDA. De igual forma las salidas de los equipos son entregados previa autorización de la Subdirección Administrativa de la Entidad y del firmado de los formatos pertinentes y registros de salida por parte de la compañía de seguridad".*

Validación de la OCI:

Lo justificado no garantiza la subsanación de la situación observada en el desarrollo del seguimiento por lo cual se mantiene la recomendación dada en el documento preliminar

- De conformidad con lo observado en el Plan de Tratamiento de los Riesgos COVID 19; aún se encuentran actividades en proceso (de un total de 57 actividades se observa que el 37% no se encuentran implementadas y el 19% se encuentran implementadas parcialmente), sobre las cuales se recomienda fortalecer la gestión que se ha venido desarrollando, en aras de garantizar el tratamiento adecuado de los riesgos ya identificados y de tal manera que los controles sean oportunos dentro del estado de emergencia que motiva el presente informe.

  A través de correo electrónico de fecha 09/07/2020 la OTIC realiza la siguiente aclaración sobre el documento preliminar:

  > *"Las actividades para el tratamiento de riesgos ante el COVID se encuentran implementados, se tiene presente que las actividades de implementación para su correcto funcionamiento demandan cambios y procedimientos que tienen que implementarse paulatinamente para que no afecten ni impacten a los funcionarios ni la entidad. De igual manera se han implementado el monitoreo y los controles de seguridad y se realizan las actualizaciones liberadas por los proveedores de servicios de seguridad como EndPoint para riesgo interno, Firewall para riesgo externo, WAF para supervisar y filtrar o bloquear tráfico HTTP hacia y desde una aplicación web y mediante el SOC que es una central de seguridad informática contratada por la SDM que previene, monitorea y controla la seguridad en las redes y en Internet; de esta manera subsanar fallas de seguridad que se pudieran presentar ante el trabajo en casa.*
  >
  > *Plan de Tratamiento de los Riesgos COVID 19 se enmarca dentro del plan general de tratamiento de riesgos que se tiene para la Entidad implementado en la plataforma en la nube Global Suite, se recalca que estos controles tienen prevista una implementación que se está dando gradualmente con el aval de la SDM y que tiene un cronograma con actividades en línea de tiempo y algunos en muchos casos requieren la consecución de recursos para su mitigación o necesitan de la definición de planes de trabajo detallados e información por parte de otras áreas y/o proveedores con los que se trabajara en el momento de su incorporación de acuerdo al plan. Se pretende continuar avanzado conforme sea posible para minimizar dicho impacto y llegar al 100% de la implementación.*

Es claro que un proceso de Gestión de Riesgos es un proceso continuo y dinámico que se ve alterado por las factores internos y externos de la organización, por lo que, una de sus etapas esenciales es el monitoreo y la supervisión, que permiten la identificación y el registro de nuevos riesgos, así como la desaparición o el cambio de categoría de otros, en ese sentido, algunos controles inicialmente planteados han tenido que cambiarse por directriz de la entidad, la cual identifica prioridades de servicio.

Por lo anterior, y como se indicó en la reunión aclaratoria con la OCI; el nivel de obsolescencia de la Entidad de hace cuatro años, era muy alto y ante la escases de recursos para realizar una actualización y renovación inmediata, hace que la OIS, hoy OTIC defina un plan de renovación tecnológica por fases, que hasta el momento no ha finalizado; dado lo anterior y recurriendo a los recursos TI que se van incorporando a la Entidad y que permiten ir avanzando en el proceso de madurez TI, se establece los procedimientos para realizar la Gestión de continuidad, para los recursos tecnológicos de la SDM y administrados por el Operador tecnológico, para lo cual se entregaron los documentos PLAN DE CONTINUIDAD y GESTION DE CONTINUIDAD, los cuales no se oficializan institucionalmente, hasta no finalizar el proceso de actualización y renovación e incorporar cada uno de los elementos que se encuentran en curso (cambio de tableros eléctricos, cambio de ups, IPv6, entre otros); Este plan logístico nos ha permitido sortear recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas en tiempos y con acciones razonables después de un incidente no deseada o desastre, como se ha podido evidenciar ante la emergencia Covid;

Sin embargo, dados los procesos de renovación y niveles de madurez TI que se han logrado; La OTIC para el cuatrienio, tiene previsto establecer los planes de continuidad del negocio y plan de contingencia los que implican un trabajo con la alta dirección y cada uno de los procesos de la entidad para definir el conjunto de procedimientos alternativos a la operatividad normal, que permitan restablecer la gestión ante cualquier desastre. Por lo anterior, se solicita se evalúe que esta acción no debe estar sujeta a un plan de mejoramiento toda vez, que está dentro de la línea del tiempo trazada por la OTIC para llegar al punto de formalizar el plan de continuidad y establecer e implementar de manera adecuada un plan de contingencia."

Validación de la OCI:

De acuerdo a los argumentos expuestos por el proceso, la OCI precisa que es evidente la gestión que adelanta la OTIC respecto al tratamiento de los riesgos identificados; no obstante, la recomendación realizada corresponde a fortalecer las acciones que hasta ahora se ha venido desarrollando de tal manera que se garantice el cumplimiento integral de las actividades de control previstas en el plan de tratamiento. Conforme lo anterior se mantiene la recomendación aclarando que corresponde al proceso evaluar la pertinencia de suscribir plan de mejoramiento de la misma, sin que este afecte la programación a ejecutar en el cuatrenio en consideración de lo indicado en la justificación entregada.

De acuerdo con los resultados obtenidos y con el fin de establecer oportunidades de mejora, se solicita a la Oficina de Tecnologías de la Información y Comunicaciones, suscribir el plan de mejoramiento correspondiente, de conformidad con lo establecido en el Procedimiento para la Formulación y Seguimiento de Planes de Mejoramiento (PV01-PR01).

Nombre(s) y firma(s) auditor(es):	Nombre y firma del Jefe de la Oficina de Control Interno
MARIA JANNETH ROMERO MARTÍNEZ	10/07/2020 X Diego Nairo Useche Rueda - DNUR Jefe Oficina de Control Interno - OCI Firmado por: Diego Nairo Useche Rueda **DIEGO NAIRO RUEDA USECHE**