INFORME DE SEGUIMIENTO

GESTIÓN DEL RIESGO DE LA SECRETARÍA DISTRITAL DE LA MUJER

PROCESO GESTIÓN TECNOLÓGICA

OFICINA DE CONTROL INTERNO

Norha Carrasco Rincón
JEFA DE LA OFICINA DE CONTROL INTERNO

EQUIPO AUDITOR
Claudia Cuesta Hernández

PERIODO EVALUADO
Enero – Noviembre 2020

FECHA DEL INFORME
Diciembre de 2020

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL 3
1.1. DESTINATARIOS 3
1.2. EQUIPO AUDITOR 3
1.3. PERIODO DE DESARROLLO DEL SEGUIMIENTO 3
2. OBJETIVOS DEL SEGUIMIENTO 3
3. ALCANCE DEL SEGUIMIENTO 4
4. CRITERIOS DEL SEGUIMIENTO 4
5. METODOLOGÍA 4
5.1. Análisis del Seguimiento y Monitoreo realizado por el Proceso a Riesgos y Controles **4**
5.2. Definición estructural del riesgo **5**
5.3. Idoneidad del diseño de controles **6**
5.4. Ejecución de controles **7**
5.5. Calificación individual y evaluación del conjunto de controles **7**
5.6. Análisis del Plan de Contingencia **8**
5.7. Resultado del seguimiento **9**
6. DESARROLLO DEL SEGUIMIENTO 10
6.1. ANÁLISIS DEL SEGUIMIENTO Y MONITOREO REALIZADO POR EL PROCESO A RIESGOS Y CONTROLES 10
6.2. ANÁLISIS DE RIESGOS DE GESTIÓN 11
6.2.1. Análisis de controles del riesgo 1 "Caídas de red (Comunicaciones, Internet, Sistemas)". **13**
6.2.2. Análisis de controles del riesgo 2 "Pérdida de Información confidencial". **14**
6.2.3. Análisis de controles del riesgo 3 "Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad". **16**
6.3. ANÁLISIS DE RIESGOS DE CORRUPCIÓN 17
6.3.1. Análisis de controles del riesgo de corrupción **18**
6.4. ANÁLISIS DEL PLAN DE CONTINGENCIA 20
7. CONCLUSIONES 21
7.1. FORTALEZAS 21
7.2. OPORTUNIDADES DE MEJORA 21
7.3. HALLAZGOS 22

1. INFORMACIÓN GENERAL

1.1. DESTINATARIOS

Las (os) lideresas (líderes) de los respectivos procesos de la Secretaría Distrital de la Mujer, como responsables de los siguientes aspectos, de conformidad con lo establecido en la Política de Administración del Riesgo de la Secretaría Distrital de la Mujer:

- Identificar y valorar los riesgos de su proceso.
- Definir controles, aplicarlos y hacer el respectivo seguimiento.
- Identificar las acciones preventivas y planes de contingencia requeridos para administrar los riesgos de su proceso, según sea el caso.
- Desarrollar ejercicios de auto evaluación frente a la administración de riesgos.
- Realizar los reportes de seguimiento de la administración de riesgos de su proceso, de conformidad con las instrucciones de la Oficina Asesora de Planeación y la Oficina de Control Interno.

1.2. EQUIPO AUDITOR

La auditora asignada para el desarrollo del presente seguimiento es Claudia Cuesta Hernández, profesional especializado de la Oficina de Control Interno.

1.3. PERIODO DE DESARROLLO DEL SEGUIMIENTO

El presente seguimiento se desarrolló de conformidad con la metodología que se detalla en el numeral 5, atendiendo a lo indicado en el numeral 6.3 "Evaluación Independiente a la Administración del Riesgo" de la Política de Administración del Riesgo de la Secretaría Distrital de la Mujer, que estable que la Oficina de Control Interno debe *"Realizar la evaluación independiente sobre la aplicación de la Política de Administración del Riesgo de la Secretaría Distrital de la Mujer,* ***en el último trimestre de cada vigencia****"* (resaltado fuera de texto) y el Plan Anticorrupción y de Atención a la Ciudadanía de la entidad, que incluye dentro de las actividades del componente "Gestión del Riesgo de Corrupción - Mapa de Riesgos de Corrupción" las realización del seguimiento a la gestión de riesgos asociados a corrupción, a desarrollarse entre septiembre y diciembre de la presente vigencia:

De esta forma, se inicia con la etapa de planeación en el mes de noviembre de 2020, y se procedió a descargar el reporte de riesgos vigentes del módulo "Riesgos y oportunidades" del aplicativo del Sistema de Gestión LUCHA, con corte del 13 de noviembre de 2020, para proceder a la realización del análisis correspondiente con base en lo consignado en el mencionado aplicativo, realizar las pruebas de recorrido que fueron necesarias y, finalmente determinar las conclusiones del seguimiento realizado.

El análisis y conclusiones fueron consolidadas en un informe por proceso, que fue entregado durante el mes de diciembre de 2020 a las(os) lideresas(es) de los respectivos procesos.

2. OBJETIVOS DEL SEGUIMIENTO

Realizar el seguimiento a la gestión del riesgo llevada a cabo por los procesos de la Secretaría Distrital de la Mujer, de acuerdo con las orientaciones de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas proferido por el Departamento Administrativo de la Función Pública (Versión 4).

3. ALCANCE DEL SEGUIMIENTO

Se realiza el seguimiento a las etapas de identificación, análisis, y evaluación de los riesgos identificados y gestionados por la Secretaría Distrital de la Mujer para el periodo comprendido entre enero y noviembre de 2020.

4. CRITERIOS DEL SEGUIMIENTO

- ✓ Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Riesgos de Gestión, Corrupción y Seguridad Digital, proferido por el Departamento Administrativo de la Función Pública (Versión 4 de octubre de 2018).
- ✓ Política de Administración del Riesgo para la Secretaría Distrital de la Mujer (Versión 3 del 29 de mayo de 2020).

5. METODOLOGÍA

En concordancia con los lineamientos proferidos desde el Departamento Administrativo de la Función Pública en la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Riesgos de Gestión, Corrupción y Seguridad Digital (Versión 4 de octubre de 2018),* se lleva a cabo el presente seguimiento a la gestión del riesgo realizada por los procesos institucionales y, a la vez, la evaluación de su tratamiento, mediante la revisión de las etapas de identificación, análisis y evaluación, haciendo énfasis en la evaluación del diseño y aplicación de los controles, tendiente a fortalecer el enfoque preventivo sobre los posibles eventos que puedan afectar el cumplimiento de los objetivos institucionales.

La metodología para la evaluación y el seguimiento a realizar inicia con el análisis de la estructura de los riesgos formulados en cuanto a las causas, las consecuencias y su tipología, determinando la coherencia entre dichos elementos y la relación del riesgo con el objetivo y el ciclo PHVA del correspondiente proceso. Luego, y teniendo en cuenta el análisis inicial se realiza la evaluación y valoración de los controles identificados para cada riesgo, determinando la idoneidad de su diseño y las condiciones de su aplicación a lo largo de la presente vigencia, para que con el análisis de estos parámetros de diseño y ejecución sea posible estimar la solidez de los controles.

De esta forma, con el ánimo de desarrollar el presente análisis, se aplican instrumentos en cada etapa (numerales 5.1, 5.2 y 5.3. del presente informe), con el propósito de identificar fortalezas y oportunidades de mejora para la gestión del riesgo y la aplicación de sus respectivos controles.

5.1. Análisis del Seguimiento y Monitoreo realizado por el Proceso a Riesgos y Controles

De acuerdo con los lineamientos establecidos desde la Política de Administración del Riesgo, las lideresas del proceso deben llevar a cabo la revisión y seguimiento cuatrimestral de sus respectivos riesgos y mecanismos de tratamiento (controles, acciones preventivas y planes de contingencia), por lo que dentro del presente informe se realiza el análisis correspondiente, con base en las respectivas actas de seguimiento y monitoreo construidas por cada proceso con corte a 31 de agosto de 2020.

Para tal fin, se revisará que en el marco del seguimiento realizado se dé respuesta a las siguientes preguntas orientadoras:

Tabla 1. Preguntas Orientadoras Seguimiento Realizado por el Proceso	
Preguntas Orientadoras	**Elementos Asociados**
✓ ¿Es necesario incluir, eliminar o actualizar riesgos?	Referencia a cada riesgo analizado, causas y consecuencias
	¿Aún es pertinente? Análisis de coherencia en relación con el proceso
	Mención y seguimiento de acciones preventivas (si se plantearon)
	¿Se materializó el riesgo? SÍ: describir situación + Plan de contingencia o acciones desarrolladas / NO: Dejar explicito
✓ ¿Es necesario incluir, eliminar o actualizar control?	Referencia a los controles y su forma de implementación
	¿Son coherentes con el riesgo y sus causas?
	¿Son efectivos? Detectivo: se detectan causas o materialización del riesgo / Preventivo: previene que se presenten causas del riesgo
	Se identifica como punto de control en procedimientos

En sentido se dan las recomendaciones del caso para la mejora continua en los ejercicios de autocontrol para la administración del riesgo realizados por los procesos de la entidad.

5.2. Definición estructural del riesgo

Se realiza un análisis de coherencia entre las causas y efectos identificados para el riesgo y su relación con los elementos de la caracterización de cada proceso, para lo cual se utilizan las siguientes preguntas como parte de dicho análisis:
¿Las causas son coherentes con el riesgo?
¿Las consecuencias son coherentes con las causas y el riesgo?
¿Con cuáles verbos clave del objetivo del proceso se relaciona?
¿El riesgo se relaciona con el objetivo del proceso?
¿La categoría (tipología) del riesgo corresponde a la definición dada en la Guía Metodológica de la Función Pública?
¿La categoría (tipología) del riesgo es coherente con las consecuencias de la materialización del riesgo?

Para facilitar este análisis se utiliza la técnica de metalenguaje, en el que se utilizan palabras intermedias para unir en una sola frase los diferentes componentes de la estructura del riesgo, como se resume en la siguiente tabla.

Tabla 2. Resumen de metalenguaje para evaluación de la estructura del riesgo					
Objetivo del proceso					
Debido a	Causa 1 Causa 2 … Causa n	**puede suceder que**	Riesgo	**lo que puede generar**	Consecuencia 1 Consecuencia 2 … Consecuencia 3

Para los riesgos asociados a corrupción, la evaluación de la estructura del riesgo se realiza teniendo en cuenta que deben concurrir dentro de su redacción los siguientes componentes: una acción u omisión + el uso del poder + la desviación de la gestión de lo público + un beneficio privado.

Con base en este análisis, esta Oficina construye observaciones sobre la redacción del riesgo y su definición estructural, partiendo desde la caracterización y su objetivo, siguiendo así las características establecidas desde el

modelo de operación por procesos, buscando la generación del valor esperado para cumplir con los objetivos institucionales y la misión de la entidad.

5.3. Idoneidad del diseño de controles

Para identificar si las características de los controles asociados a los riesgos reúnen las condiciones necesarias para mitigarlos, se revisa el cumplimiento de los criterios establecidos en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas", con el ánimo de valorar la idoneidad del diseño de los controles. En la tabla 3 se resumen estos criterios:

Tabla 3. Cuadro resumen de la evaluación de la idoneidad del diseño de controles

Criterio de evaluación	Aspecto	Opciones y peso de respuesta		
1. Responsable	¿Existe un responsable asignado para la ejecución del control?	Asignado		No Asignado
		15		0
	¿El responsable tiene la autoridad y adecuada segregación de funciones para la ejecución del control?	Adecuado		Inadecuado
		15		0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna		Inoportuna
		15		0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir		Detectar
		15		10
4. Cómo se realiza la actividad de control	¿Se establece el manejo que se debe dar a las desviaciones u observaciones resultantes de la ejecución del control?	Definido	Incompleto	No definido
		18	8	0
5. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta	No existe
		15	5	0
	¿El control está documentado y formalizado en LUCHA?	SI		NO
		7		0
Total calificación peso respuestas		**100**		

NOTA. La metodología del DAFP recomienda ciertas calificaciones para la evaluación del control; sin embargo, y de acuerdo con el nivel de madurez de la gestión del riesgo en la Entidad, se realizó un ajuste en las ponderaciones dadas a cada criterio de evaluación.

Es de aclarar que si del análisis realizado se concluye que el control formulado por el proceso NO es un control[1], las demás variables de diseño y ejecución no serán objeto de evaluación.

En concordancia con los resultados obtenidos de la evaluación del diseño del control se da un rango de calificación entre fuerte, moderado y débil, como se muestra en la tabla 4.

[1] Para los controles preventivos se analiza si existe relación directa entre el control y la disminución de la probabilidad de ocurrencia del riesgo. Para los controles detectivos se analiza si existe relación entre el control y la disminución del impacto cuando ya se ha materializado el riesgo.

Tabla 4. Cuadro resumen de calificación del diseño del control	
Rango de calificación	**Resultado peso evaluación del control**
Fuerte	Calificación entre 95 y 100
Moderado	Calificación entre 86 y 94
Débil	Calificación entre 0 y 85

Como se puede detallar en la tabla 4, el traslado a términos cualitativos de la calificación obtenida para el diseño del control es exigente desde el punto de vista cuantitativo; esto se sustenta en el impacto que puede tener la materialización de un riesgo en el cumplimiento del propósito del proceso y, en consecuencia, de los objetivos de la Entidad.

5.4. Ejecución de controles

Para evaluar la ejecución de controles se tiene en cuenta tanto la aplicación del control de conformidad con su diseño, como la manera en que este se evidencia en desarrollo de los procedimientos de los procesos y las funciones asignadas.

Adicionalmente, se analiza si se ha materializado el riesgo, o existen hallazgos u observaciones de auditoría relacionados con el riesgo y la aplicación del control, información que constituye los antecedentes sobre el tema, y que complementa el análisis realizado.

En la tabla 5 se resume la forma de realizar esta calificación, y la conclusión asociada a cada tema.

Tabla 5. Cuadro resumen de calificación de la ejecución de controles	
Rango de calificación	**Resultado peso ejecución del control**
Fuerte	El control se ejecuta de manera consistente por parte del responsable NO se ha materializado el riesgo o NO existen hallazgos u observaciones de auditoría.
Moderado	El control se ejecuta de manera consistente por parte del responsable SI se ha materializado el riesgo o SI existen hallazgos u observaciones de auditoría.
	El control se ejecuta algunas veces por parte del responsable NO se ha materializado el riesgo o NO existen hallazgos u observaciones de auditoría.
Débil	El control se ejecuta algunas veces por parte del responsable SI se ha materializado el riesgo o SI existen hallazgos u observaciones de auditoría.
	El control no se ejecuta por parte del responsable, independientemente de su materialización y la existencia o no de hallazgos de auditoría

Como se puede detallar en la tabla 5, la calificación de la ejecución es exigente, en el sentido de que sólo se puede tener una calificación “Fuerte”, cuando se aplique de manera consistente el control y no existan antecedentes de materialización del riesgo, o hallazgos u observaciones de auditoría.

5.5. Calificación individual y evaluación del conjunto de controles

Una vez se tiene la evaluación de cada control en su diseño y su ejecución, se determina la evaluación individual del control y la evaluación del conjunto de controles, de conformidad con lo consignado en la tabla 6.

Tabla 6. Cuadro resumen de calificación individual del control del conjunto de controles			
Calificación del diseño	**Calificación de la ejecución**	**Calificación individual**	**Calificación del conjunto de controles**
Fuerte	Fuerte	Fuerte = 100	Determinar el promedio de la calificación individual. Fuerte: igual a 100. Moderado: mayor o igual a 50 y menor a 100. Débil: menor a 50.
	Moderado	Moderado = 50	
	Débil	Débil = 0	
Moderado	Fuerte	Moderado = 50	
	Moderado	Moderado = 50	
	Débil	Débil = 0	
Débil	Fuerte	Débil = 0	
	Moderado	Débil = 0	
	Débil	Débil = 0	

Como se puede detallar, la calificación individual es exigente, toda vez que se da más peso a la calificación más baja entre diseño y ejecución. Esta situación se ve reflejada al calificarse el conjunto de controles, pues la única opción para que dicha calificación sea "Fuerte" se presenta cuando la totalidad de los controles asociados a un riesgo tiene esta misma calificación.

Por tal motivo, si bien se entrega el resultado de la calificación individual y del conjunto de controles, se tomarán como base para el análisis y las recomendaciones, las evaluaciones de su diseño y ejecución.

5.6. Análisis del Plan de Contingencia

El *Plan de Contingencia* para llevar a cabo el tratamiento de un riesgo, corresponde a un plan de acción en el que se establecen las acciones a seguir en caso de su materialización, y parte de la identificación y priorización de escenarios de riesgo para formular medidas adicionales a las existentes.

De esta forma, se realiza el análisis correspondiente en concordancia con lo señalado en la Política de Administración del Riesgo de la Secretaría Distrital de la Mujer, por medio de la cual se establecen los niveles de aceptación y manejo de los riesgos de gestión (estratégicos, financieros, de cumplimiento, operativos, de imagen y ambientales) y de seguridad de la información, así:

Tabla 7. Aceptación del Riesgo con Opciones de Tratamiento Política de Administración del Riesgo Secretaría Distrital de la Mujer		
Zona de riesgo	**Aceptación del riesgo**	**Opción de tratamiento**
Bajo	SI	Definición e implementación de controles.
Moderada	SI	Definición e implementación de controles.
Alta	NO	Definición e implementación de controles y acciones preventivas.
Extrema	NO	Definición e implementación de controles, acciones preventivas y plan de contingencia.

Fuente: Política de Administración del Riesgo Versión 3 Secretaría Distrital de la Mujer

Lo anterior es coherente con las recomendaciones y mejores prácticas para la administración del riesgo, en las que se definen los niveles de aceptación, de la siguiente forma[2]:

[2] Fuente: Política de Administración del Riesgo Versión 3 Secretaría Distrital de la Mujer

1. Zona de riesgo bajo: se acepta el riesgo.
2. Zona de riesgo moderada: se acepta el riesgo.
3. Zona de riesgo alta: no se acepta el riesgo, se reduce, se evita, o se comparte.
4. Zona de riesgo extrema: no se acepta el riesgo, se reduce, se evita y se comparte.

Para la evaluación del plan de contingencia se tendrán en cuenta aspectos como:

- Área o proceso afectado.
- Causa de la contingencia analizada y si es coherente con la causa raíz del riesgo,
- Si se ha llegado a desarrollar el plan formulado, cuál ha sido el efecto y si fue efectiva la activación de dicho plan.

En este sentido se identifican cuáles riesgos contenidos en las matrices de cada uno de los procesos se encuentran en zona extrema, y de acuerdo con lo consignado en el módulo "Riesgos y oportunidades" del aplicativo del Sistema de Gestión LUCHA, se establecen las observaciones y recomendaciones sobre los planes de contingencia formulados. También se identificarán las oportunidades de mejora pertinentes para los procesos que no hayan realizado aún el ejercicio correspondiente.

5.7. Resultado del seguimiento

Con la información analizada y consolidada en el marco de los criterios del seguimiento (numeral 4), se construyen las conclusiones del informe de seguimiento mediante la identificación de fortalezas y debilidades; estas últimas, a su vez, están compuestas por dos tipos, las oportunidades de mejora y los hallazgos, cuyas definiciones se detallan a continuación:

- **Oportunidad de mejora**: Hace referencia a la identificación de temas problemáticos y mejoras potenciales sobre una situación específica identificada a lo largo del proceso auditor. Dicha situación puede llegar a ser reiterativa y podría llegar a tener efectos sobre el cumplimiento de los objetivos de los procesos institucionales, por lo que es necesario identificarlas, analizarlas y tomar decisiones sobre su tratamiento. En caso de que, producto de análisis realizado, el proceso determine que se acogerán las oportunidades de mejora y se tomen medidas para su tratamiento, las mismas deberán documentarse en el correspondiente plan de mejoramiento.

- **Hallazgo de auditoría**: Es un hecho relevante que se constituye en un resultado determinante en la evaluación de un proceso o un asunto en particular, al realizar la comparación de La Condición (situación detectada o hechos identificados) con El Criterio que se refiere al deber ser (cumplimiento de normas, reglamentos, lineamientos o procedimientos); y además para mayor claridad se complementa estableciendo sus Causas (qué originó la diferencia encontrada) y Efectos (situaciones adversas que pueden ocasionar la diferencia encontrada). Los hallazgos deben ser objeto de formulación de acciones tendientes a eliminar de fondo las causas que las originaron, las cuales harán parte del correspondiente plan de mejoramiento.

Cabe aclarar que el término "**Plan de Mejoramiento**" hace referencia al instrumento que recoge y articula todas las acciones prioritarias que se emprenderán para mejorar aquellas características que tendrán mayor impacto en los resultados esperados, el logro de los objetivos de la entidad y la ejecución del plan de acción institucional. Su objetivo primordial es promover que la gestión de la entidad se desarrolle en forma eficiente y transparente, a

través de la adopción y cumplimiento de las acciones correctivas y/o de la implementación de metodologías orientadas al mejoramiento continuo.

Para finalizar, se precisa que la formulación de las acciones preventivas, correctivas y de mejora, producto de cualquier tipo de ejercicio auditor, deben formularse dentro de los quince (15) días hábiles siguientes a la presentación del Informe de Seguimiento y/o Auditoria y estas deben ser consignadas en el módulo de mejoramiento continuo del aplicativo LUCHA para su ejecución, monitoreo y seguimiento. Asimismo, la Oficina de Control Interno, realizará el seguimiento correspondiente sobre el avance de las acciones planteadas, además de efectuar el análisis y verificación de la efectividad alcanzada en este proceso.

6. DESARROLLO DEL SEGUIMIENTO

6.1. ANÁLISIS DEL SEGUIMIENTO Y MONITOREO REALIZADO POR EL PROCESO A RIESGOS Y CONTROLES

A través de reunión virtual realizada por el equipo de trabajo de la Oficina Asesora de Planeación para la Gestión Tecnológica, se llevó a cabo el monitoreo y seguimiento correspondiente sobre la administración de los riesgos formulados con corte al de mes de agosto de la presente vigencia; de la cual se observa que fue elaborada el acta de autoevaluación sobre el tema con fecha 02 de septiembre de 2020, con el fin de realizar la revisión y seguimiento cuatrimestral de los riesgos y mecanismos de tratamiento para el proceso de gestión tecnológica.

1. **Análisis de Coherencia entre Riesgos y la Caracterización del Proceso:** En el marco de la mejora continua sobre la gestión de la entidad, se observa que el proceso "Gestión tecnológica" llevó a cabo la actualización de la caracterización y la revisión de sus documentos asociados, ejercicio a partir del cual se realizó el análisis pertinente sobre la relación entre el objetivo del proceso y cada uno de los riesgos planteados. De dicho ejercicio, el acta en mención indica que los cuatro (4) riesgos del proceso están articulados con lo definido desde el objetivo planteado en la versión actualizada del documento de *"Caracterización del Proceso de Gestión tecnológica GT-CA-01 Versión 3 del 16 de julio de 2020".*

2. **Análisis de Causas – Riesgo y Consecuencias:** Se evidencia dentro de lo consignado en el acta de autoevaluación, que el proceso "Gestión tecnológica" realizó los análisis correspondientes para cada caso, determinando para el riesgo de caída de red la necesidad de ajustes y/o eliminación en algunas de sus causas y para los demás riesgos se concluyó no se requieren cambios dado que existe coherencia entre causas y consecuencias identificadas. Las mejoras y los ajustes realizados fueron evidenciados dentro de la información consignada en el aplicativo LUCHA.

3. **Ejecución y Efectividad de los Controles***:* El ejercicio de autoevaluación realizado por el proceso también incluyó el análisis de eficacia y efectividad de los controles formulados para sus riesgos, mediante la identificación de rastros de su aplicación y sus correspondientes evidencias de los registros indicados en los procedimientos de gestión tecnológica. Además, se observa que el proceso realizó cambios en los controles del riesgo *Perdida de Información confidencial,* quedando estructuradas 4 actividades como parte del tratamiento de dicho riesgo; para los otros riesgos se evidencia que el proceso continuó con los mismos controles que se habían identificado anteriormente concluyendo que estos siguen siendo efectivos para su tratamiento.

4. **Revisión estructura riesgo asociado a corrupción:** El proceso de Gestión Tecnológica ejecutó la autoevaluación correspondiente sobre todos los elementos del riesgo de corrupción formulado, de lo cual

se registró el análisis de coherencia del riesgo con el objetivo del proceso en concordancia con los cambios realizados a la caracterización, y la revisión correspondiente con el cumplimiento de los componentes de la definición como riesgo asociado a corrupción.

5. **Identificación de materialización de riesgos:** El proceso "Gestión tecnológica" indica en el acta de autoevaluación a la administración de sus riesgos, que durante la presente vigencia no se ha dado la materialización de ninguno de sus riesgos.

6. **Otras situaciones:** En el acta revisada también se hace referencia a ciertos cambios realizados sobre la aplicación de los controles formulados para mitigar los riesgos, en cuanto a la situación coyuntural que se tiene en el momento en relación con la cuarentena establecida y el trabajo en casa debido a la pandemia, por lo que se han tomado medidas específicas y se ha dado manejo a las desviaciones para el uso de controles.

De acuerdo con lo anterior, se evidencia que el proceso "Gestión tecnológica" llevó a cabo el ejercicio de autoevaluación y monitoreo a la gestión de sus riesgos, teniendo en cuenta las preguntas orientadoras dadas como lineamiento genérico para registrar la mejora continua en cuanto a incluir, eliminar o actualizar riesgos y controles. No obstante, se observa que en revisión del acta elaborada por el proceso evaluado, no se registran análisis sobre el tratamiento de los riesgos formulados en cuanto a planes de contingencia y acciones preventivas; esto dado que los riesgos inherentes del proceso se encuentran en zona alta y extrema y que en línea con lo establecido por la Política de Administración del Riesgo de la SDMujer en su punto No. 7 *Niveles de Aceptación y Tratamiento del Riesgo,* es necesario formular como parte del tratamiento no solo controles sino también planes de contingencia y acciones preventivas.

6.2. ANÁLISIS DE RIESGOS DE GESTIÓN

Los riesgos de gestión asociados al proceso "Gestión Tecnológica" se presentan en la Tabla 8.

Tabla 8. Riesgos de gestión del proceso "Gestión Tecnológica"
Estructura del riesgo

Objetivo del proceso: Planificar, gestionar, evaluar y optimizar la infraestructura tecnológica, que responda a los requerimientos solicitados por parte de los usuarios de la Secretaría Distrital de la Mujer, con el fin de garantizar la seguridad y la continuidad de la infraestructura tecnológica y velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información; garantizando un servicio eficiente en las tecnologías de la información y las comunicaciones.

	Causas		Descripción del riesgo		Consecuencias
Debido a	Daño de Equipos de comunicaciones. Daño en servidores. Daño en Aplicativos. Daño del Sistema de alimentación interrumpida (UPS). El no pago de los servicios. Errores humanos. Falta de mantenimientos preventivos y correctivos a los equipos de comunicaciones, servidores y eléctricos. Redundancia de equipos de comunicaciones.	***puede suceder que***	**Riesgo 1.** Caídas de red (Comunicaciones, Internet, Sistemas) Riesgo Tecnológico	***lo que puede generar***	Retrasos y dificultades en las labores de las servidoras y servidores de la Entidad. Incumplimientos de las obligaciones de la entidad. Pérdida de información.

Tabla 8. Riesgos de gestión del proceso "Gestión Tecnológica" Estructura del riesgo					
Debido a	Caídas de los servidores. Manipulación de la información. Falta de backup (respaldo externo). Préstamo de usuarios y contraseñas. Falta de seguridad Perimetral. Accesos no autorizados al centro de cómputo. Falta de seguridad física del centro de cómputo (acceso, aire, detectores de incendio, etc). Daño físico de discos duro (Servidores y Almacenamiento). Segmentación de red servicios internos.	***puede suceder que***	**Riesgo 2.** Pérdida de Información confidencial Riesgo Tecnológico	***lo que puede generar***	Retrasos y dificultadas en las labores de las servidoras y servidores de la Entidad. Reportes erróneos. Duplicidad de la información. Bajos niveles de seguridad en la información. Retrasos en el procesamiento de datos por la necesidad de verificar y depurar la información.
Debido a	Falta de herramientas para el control de la seguridad de la información. Falta de actualización de credenciales de usuarios de los diferentes aplicativos y sistemas de información. Préstamo de la clave de acceso.	***puede suceder que***	**Riesgo 3**. Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad. Riesgo Tecnológico	***lo que puede***	Se favorece el fraude y el soborno Impide la ejecución exitosa de otros procesos y afecta la competitividad de la entidad. Incide en la calidad de la información, en la agilidad, costos y credibilidad en cuanto a los procedimientos y seguridad de los mismos.

Teniendo en cuenta la metodología descrita en el numeral 5.2 del presente informe, en relación con la estructura de los riesgos identificados se puede concluir lo siguiente:

1. Genéricamente se evidencia qué para lo relacionado con la definición de los riesgos formulados por el proceso de gestión tecnológica, aplicando la metodología del metalenguaje, la relación entre los elementos causa – riesgo – consecuencia es coherente y corresponde consecuentemente con lo establecido en la caracterización del proceso.

2. En cuanto a la tipología indicada como riesgo tecnológico, se observa que es conforme con los eventos que se pueden presentar a lo largo de la operación del proceso y se articula con las consecuencias expuestas para cada riesgo.

3. En revisión de la coherencia entre los elementos de la caracterización del proceso de Gestión Tecnológica y la definición de sus riesgos se observa que existe relación con lo descrito en los verbos clave del objetivo del proceso y adicionalmente se identifican los eventos dentro de las actividades descritas en el ciclo PHVA, sobre todo en las etapas del PLANEAR, HACER Y VERIFICAR. (Ver Anexo 1).

4. Por otro lado, se observa que dentro del *Manual de Políticas Específicas de Seguridad de la Información* con código *GT-MA-3*, en el marco de sus objetivos se establece *"Cubrir los 14 dominios de seguridad de la información y sus controles, conforme a lo que indica la NTC ISO 27001:2013"* y en este sentido es importante recomendar que se articule la administración del riesgo del proceso de Gestión Tecnológica con lo consignado a lo largo del manual, sobre todo en lo que respecta al tratamiento de los riesgos ya que desde los dominios de seguridad de la información se establecen controles específicos en cuanto a la mitigación de posibles eventos que afecten el cumplimiento del objetivo del proceso. Adicionalmente, es importante acotar que es necesario llevar a cabo la articulación correspondiente del mapa de riesgos establecido por el proceso de Gestión Tecnológica, con todos los lineamientos señalados en el documento con el fin de fortalecer la administración de los riesgos de seguridad de la información en la entidad.

5. El objetivo de seguridad de la información "*Lograr la protección de la Información física y digital, el hardware, el software, aplicativos, servicios, redes de datos y comunicaciones, por medio de la divulgación, conocimiento, apropiación y cumplimiento del Manual de Políticas Específicas de Seguridad de la Información."* (el cual se encuentra armonizado dentro de la Política de Seguridad de la Información de la SDMujer V3 de julio de 2020), puntualiza que la información, el software y el hardware son elementos operacionales para el proceso en evaluación, por lo que es recomendable analizar la existencia de riesgos asociados al hardware, dado que los riesgos formulados por el proceso hacen referencia a la información y al software.

6. Se retoma la observación dada por este despacho en informes anteriores en cuanto a la articulación con la implementación de la *Política de Gobierno Digital (Manual Técnico MIPG)*, dado que es necesario que se realice un análisis sobre la formulación de un riesgo relacionado con el atributo de *Privacidad de la Información* que se define dentro del habilitador transversal de seguridad de la información de dicha política. Aunque se tiene un riesgo sobre Pérdida de la Información Confidencial, es necesario determinar si podrían existir otros eventos que afectarían la privacidad de la información, no solo la que se considera según la ley como *"Confidencial*".

7. En cuanto al tratamiento de los riesgos del proceso, de acuerdo con lo consignado en el módulo de riesgos y oportunidades del aplicativo LUCHA, se recomienda formular acciones preventivas que articuladamente con los controles y el plan de contingencia completen el plan de tratamiento, de conformidad con los lineamientos proferidos desde el numeral 7 de la Política de Administración del Riesgo para los niveles de aceptación y tratamiento de los riesgos.

6.2.1. Análisis de controles del riesgo 1 "Caídas de red (Comunicaciones, Internet, Sistemas)".

Este riesgo cuenta con 2 controles a los cuales se realizó la evaluación de diseño y ejecución, dando como resultado que en su conjunto estos controles tienen una solidez débil, como se resume en la Tabla 9 (el detalle se encuentra en el Anexo 1).

Tabla 9. Resumen de calificación de controles – Riesgo "Caídas de red (Comunicaciones, Internet, Sistemas)".

No.	Descripción del control	Evaluaciones		Calificaciones	
		Diseño	Ejecución	Individual	En conjunto
1	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de cómputo.	**67**: Débil	Moderado	Débil	Débil
2	Establecer control de acceso al centro de cómputo	**82**: Débil	Moderado	Débil	

A continuación, se relaciona el análisis realizado para cada uno de los controles identificados por el proceso:

Control No. 1

En cuanto al diseño del control se observa que se encuentra documentado dentro *de MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3*, donde se indica el alcance del control, los responsables de llevarlo a cabo y para algunas actividades se identifica su periodicidad. Para la evaluación de la ejecución del control se observa que su aplicación corresponde una actividad que requiere de un plan de trabajo compuesto por varias acciones

puntuales para desarrollarlo, lo cual podría tornar el control en una herramienta difícil de manejar ya que necesita varios responsables para su aplicación y las diferentes acciones tienen una periodicidad variada.

Por otra parte y en lo concerniente a lo reportado dentro del aplicativo LUCHA módulo de riesgos, se recogen las observaciones dadas en informes anteriores en cuanto a que se vuelve a evidenciar que a pesar de que el control se utiliza y no cuenta con observaciones o hallazgos de auditoria, no es pertinente identificar un control que solo se pueda ejecutar cada año, esto dado que el riesgo *Caídas de red* implica un impacto muy alto sobre la gestión propia de la entidad, con unas consecuencias que podrían estar relacionadas con parar la operación de la entidad.

En este sentido, se recomienda revisar las políticas de operación y las actividades de control contenidas en los manuales y procedimientos del proceso de gestión tecnológica que tienen que ver con la planeación y puesta en marcha del plan de mantenimiento preventivo y correctivo para servidores y equipos de cómputo.

Adicionalmente, se recomienda tener en cuenta lo establecido por el procedimiento *GT-PR-16 - GESTIÓN DE SOLUCIONES Y SERVICIOS - V1,* que indica como producto el mantenimiento preventivo y correctivo a los sistemas de información de la entidad y por ende da los lineamientos correspondientes al funcionamiento de las soluciones tecnológicas; dado que para el tratamiento de este riesgo no solo se debe considerar el buen funcionamiento de los equipos de cómputo y los servidores sino también el mantenimiento necesario para los sistemas de información institucionales.

Control No. 2

Se identifica que la evaluación del diseño del control, la información consignada en el aplicativo LUCHA arroja que tiene un responsable para ejecutar la actividad y se aplica cada vez que se requiere. Se encuentra documentado dentro de los lineamientos aportados desde el *MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 y* la aplicación del formato *GT-FO-13 – REGISTRO DEL INGRESO AL CENTRO DE COMPUTO - V1* y se evidencia que no cuenta con observaciones o hallazgos de auditoria.

Para el conjunto de controles del riesgo en cuestión se observa que no se cuenta con rastro de aplicación dentro de la ejecución que se debe reportar en el aplicativo LUCHA módulo de riesgos y oportunidades. No obstante, en revisión de la herramienta se observó que el control *Establecer control de acceso al centro de cómputo* se aplica también en el riesgo asociado a corrupción y desde allí sí se cuenta con la evidencia relacionada para los primeros meses de la vigencia dada la situación de trabajo en casa, evidencia que fue consignada y reportada dentro del módulo.

6.2.2. Análisis de controles del riesgo 2 "Pérdida de Información confidencial".

Este riesgo cuenta con 4 controles a los que se les realizó la evaluación de diseño y ejecución, dando como resultado que en su conjunto los controles tienen una solidez débil, como se resume en la Tabla 10 (el detalle se encuentra en el Anexo 1).

Tabla 10. Resumen de calificación de controles – Riesgo "Pérdida de Información confidencial".

No.	Control	Evaluaciones		Calificaciones	
		Diseño	Ejecución	Individual	En conjunto
1	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	**67**: Débil	Moderado	Débil	Débil

Tabla 10. Resumen de calificación de controles – Riesgo "Pérdida de Información confidencial".

No.	Control	Evaluaciones		Calificaciones	
		Diseño	Ejecución	Individual	En conjunto
2	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	**77**: Débil	Débil	Débil	
3	Socializar la política de seguridad de la SDMujer	No es un Control	N. A.	N. A.	
4	Monitorear las amenazas que puedan vulnerar los equipos de cómputo, así como la información de la entidad	**30**: Débil	Débil	Débil	

A continuación, se relaciona el análisis realizado:

Control 1

Se consigna lo observado en el riesgo anterior, en cuanto a que el control es evaluado como débil dado que, al indicar periodos de aplicación tan largos, la pérdida de información se puede materializar en cualquier momento, a pesar de estar formalizado dentro del documentos nombrado MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3.

Control 2

El control se encuentra documentado como parte de los protocolos establecidos en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 que en su aparte 3.10 Administración de Backup y recuperación de la información, indica la política de operación para backup de los sistemas operativos, bases de datos, aplicaciones y recursos compartidos. Asimismo, se identifican los responsables de realizar los correspondientes respaldos de información y verificación de acuerdo con el tipo de elemento o recurso de almacenamiento.

En lo relacionado con el periodo de ejecución del control, el manual indica diferentes momentos en el tiempo para realizar el backup para los sistemas operativos, bases de datos, aplicaciones y recursos compartidos; lo cual difiere con lo consignado en la matriz de riesgos ya que allí se señala que esta actividad se debe llevar a cabo mensualmente. Se recomienda revisar la pertinencia del periodo de ejecución que se establece, ya que esto podría generar confusiones al momento de la aplicación del control por parte de los responsables; es así que se hace necesario analizar si se requiere ampliar el control mencionado las especificidades para los recursos de almacenamiento (sistemas operativos, bases de datos, aplicaciones y recursos compartidos)

Control 3

Se retoma la observación aportada por este despacho en varios informes y seguimientos, en cuanto a las actividades relacionadas con socializar o dar a conocer cualquier tipo de documento o información, ya que esta no corresponde a un control. Para esta acción en específico Socializar la política de seguridad de la SDMujer se observa que no es posible controlar o determinar qué tanto del tema socializado quedó interiorizado en los participantes y adicionalmente se le asigna una periodicidad muy larga para su aplicación que se podría significar un impacto significativo en caso de materialización del riesgo. Es por esto que se recomienda formular controles de carácter permanente y acordes al volumen de información que se produce continuamente en la entidad.

Para este tipo de actividades que se relacionan con talleres, socializaciones o capacitaciones sobre temas específicos o para dar a conocer normas o documentos a implementar, se recomienda analizar la posibilidad de identificarlas como acción preventiva para reforzar el tratamiento del riesgo.

Control 4

En revisión de los documentos del proceso, se identificó que la actividad indicada como control no se enuncia específicamente sobre la operación del proceso; se evidenció que dentro de los protocolos determinados en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 se contempla la gestión de incidentes de seguridad de la información de acuerdo con el tipo de incidente que llegara a presentarse y en este sentido se clasifican también el nivel de criticidad y de escalonamiento con que debe tratarse y los responsables en cada caso.

Es así que a pesar de que el control formulado no se encuentra textualmente enunciado en los documentos del proceso, se percibe que podría estar asociado con lo establecido por los lineamientos del manual de gestión tecnológica, por lo que se recomienda analizar si se requiere indicar específicamente la realización de este tipo de monitoreos y además evidenciar la periodicidad con que se requiere aplicar el control, máxime que dichos lineamientos declaran la utilización de un formato de registro de incidentes de seguridad de la información que no se encuentra formalizado en el aplicativo LUCHA.

Para el conjunto de controles del riesgo en cuestión, se observa que no se cuenta con rastro de aplicación dentro de la ejecución que se debe reportar en el aplicativo LUCHA módulo de riesgos y oportunidades. No obstante, en revisión de la herramienta se observó que el control Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer se aplica también en el riesgo 3 y desde allí si se cuenta con la evidencia relacionada para los primeros meses de la vigencia dada la situación de trabajo en casa, evidencia que fue consignada y reportada dentro del módulo.

6.2.3. Análisis de controles del riesgo 3 "Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad".

Este riesgo cuenta 2 controles a los cuales se les realizó la evaluación de diseño y ejecución (Anexo 1), dando como resultado que estos en su conjunto tiene una solidez débil, como se resume en la Tabla 11 (el detalle se encuentra en el Anexo 1).

Tabla 11. Resumen de calificación de controles – Riesgo "Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad".

No.	Control	Evaluaciones		Calificaciones	
		Diseño	Ejecución	Individual	En conjunto
1	Programar el cambio de contraseña de los usuarios cada 45 días	**100**: Fuerte	Fuerte	Fuerte	Débil
2	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	**85**: Débil	Fuerte	Débil	

A continuación, se relaciona el análisis realizado:

Control 1

La actividad identificada como control se encuentra documentada en los lineamientos aportados desde el MANUAL DE LINEAMIENTOS HERRAMIENTAS TECNOLOGICAS GT-MA-2 en su versión 1, por lo que cumple con los criterios que se designan para el diseño y se evidencia que se ejecuta de manera consistente por parte del responsable; por otro lado, no se tienen hallazgos de auditoria asociados y el riesgo no se ha materializado durante el lapso de su seguimiento actual. Se recomienda articular la periodicidad establecida en el aplicativo LUCHA (mensual) con la periodicidad descrita en el control (45 días) y asimismo con la aplicación de este mismo para el riesgo asociado a corrupción.

El proceso indica que para este periodo de evaluación y debido a la contingencia por la emergencia sanitaria, se amplió el tiempo de definido de cambio de contraseñas, con el fin de minimizar el impacto de negación de acceso a los servicios tecnológicos que están asociados a los usuarios y contraseñas de acceso. El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado.

Con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis de los puntos de control que se citan dentro de los diferentes documentos del proceso, identificando controles específicos y con una periodicidad razonable para mitigar la materialización del riesgo.

Control 2

El control se encuentra documentado como parte de los protocolos establecidos en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 que en su aparte 3.10 Administración de Backup y recuperación de la información, indica la política de operación para backup de los sistemas operativos, bases de datos, aplicaciones y recursos compartidos. Asimismo, se identifican los responsables de realizar los correspondientes respaldos de información y verificación de acuerdo con el tipo de elemento o recurso de almacenamiento. No se evidencian observaciones o hallazgos de auditoria relacionados con la aplicación del control.

En lo relacionado con el periodo de ejecución del control, el manual indica diferentes momentos en el tiempo para realizar el backup para los sistemas operativos, bases de datos, aplicaciones y recursos compartidos; lo cual difiere con lo consignado en la matriz de riesgos ya que allí se señala que esta actividad se debe llevar a cabo mensualmente. Se recomienda revisar la pertinencia del periodo de ejecución que se establece, ya que esto podría generar confusiones al momento de la aplicación del control por parte de los responsables; es así que se hace necesario analizar si se requiere ampliar el control mencionado las especificidades para los recursos de almacenamiento (sistemas operativos, bases de datos, aplicaciones y recursos compartidos).

Se cuenta con el registro de la ejecución del control de los backup realizados a los elementos de almacenamiento en los meses de abril, mayo, julio, agosto y septiembre del presente año. El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado, pero dado que el documento fue implementado recientemente no se evidencian registros sobre el particular.

6.3. ANÁLISIS DE RIESGOS DE CORRUPCIÓN

Los riesgos de corrupción asociados al proceso “Gestión Tecnológica” se presentan en la Tabla 12.

Tabla 12. Riesgos de corrupción del proceso "Gestión Tecnológica "
Estructura del riesgo

Objetivo del Proceso: Planificar, gestionar, evaluar y optimizar la infraestructura tecnológica, que responda a los requerimientos solicitados por parte de los usuarios de la Secretaría Distrital de la Mujer, con el fin de garantizar la seguridad y la continuidad de la infraestructura tecnológica y velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información; garantizando un servicio eficiente en las tecnologías de la información y las comunicaciones.

Componentes de los riesgos asociados a corrupción:
acción u omisión + uso del poder + desviación de la gestión de lo público + beneficio privado

	Causas		Riesgo		Consecuencias
Debido a	- Debilidades en la implementación de controles de acceso. - Intereses particulares de servidoras(es) públicos y/o contratistas. - Presiones indebidas u ofrecimiento de dádivas por parte de terceros	***puede suceder que***	Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad	***lo que puede generar***	Retrasos y dificultadas en las actividades operativas y misionales de la Entidad. Manipulación indebida de la información Imposibilidad de recuperar la información Alteración y/o venta de los datos e información de la Entidad y de Terceros en beneficio propio o de un tercero

Teniendo en cuenta la metodología descrita en el numeral 5.2 del presente informe, en relación con la estructura de los riesgos identificados su puede concluir lo siguiente:

1. Se evidencia que con relación a la estructura y redacción del riesgo contiene los componentes de la tipología de corrupción, como son: La acción, el uso del poder, la desviación de la gestión de lo público y el beneficio privado.
2. En cuanto a la coherencia entre el objetivo del proceso y la definición del riesgo asociado a corrupción se observa que están relacionados sobre las acciones que tienen que ver con garantizar la seguridad y la continuidad de la infraestructura tecnológica y velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información; por lo tanto, el evento se encuentra reflejado en las actividades del HACER del ciclo PHVA y se cuenta con procedimientos asociados al mismo.
3. Aplicando la metodología del metalenguaje se observa que la relación causa – riesgo – consecuencia es coherente.

Por otra parte, se observa que para el tratamiento del riesgo asociado a corrupción no se ha tenido en cuenta lo establecido desde la Política de Administración del Riesgo en su numeral 7 en cuanto a los niveles de aceptación y tratamiento, dado que por tratarse de un riesgo inherente en zona extrema se deben formular controles y acciones preventivas que ayuden a mitigar los efectos del riesgo. Las acciones indicadas dentro del aplicativo LUCHA en el ítem "*Plan de Tratamiento*" es necesario revisarlas en el marco de los lineamientos que se vayan a dar próximamente desde la Oficina Asesora de Planeación en cuanto a la asesoría técnica y metodológica que se prestará a los procesos para la administración de sus riesgos.

6.3.1. Análisis de controles del riesgo de corrupción

Este riesgo cuenta con 2 controles a los que se realizó la evaluación de diseño y ejecución, dando como resultado que el conjunto de controles tiene una solidez débil, como se resume en la Tabla 13 (el detalle se encuentra en el Anexo 1).

Tabla 13. Resumen de calificación de controles – Riesgo "Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad"					
No.	**Control**	**Evaluaciones**		**Calificaciones**	
		Diseño	**Ejecución**	**Individual**	**En conjunto**
1	Programar el cambio de contraseña de los usuarios cada 45 días	**85**: Débil	Fuerte	Débil	Débil
2	Establecer control de acceso al centro de computo	**75**: Débil	Fuerte	Débil	

A continuación, se relaciona el análisis realizado:

Control 1

La actividad identificada como control se encuentra documentada en los lineamientos aportados desde el MANUAL DE LINEAMIENTOS HERRAMIENTAS TECNOLOGICAS GT-MA-2 en su versión 1, por lo que cumple con los criterios que se designan para el diseño y se evidencia que se ejecuta de manera consistente por parte del responsable; por otro lado, no se tienen hallazgos de auditoria asociados y el riesgo no se ha materializado durante el lapso de su seguimiento actual. Se recomienda articular la periodicidad establecida en el aplicativo LUCHA (trimestral) con la periodicidad descrita en el control (45 días) y con la aplicación de este mismo para el riesgo relacionado con eliminar y modificar información en las bases de datos de los sistemas de información de la entidad.

El proceso indica que para este periodo de evaluación y debido a la contingencia por la emergencia sanitaria, se amplió el tiempo de definido de cambio de contraseñas, con el fin de minimizar el impacto de negación de acceso a los servicios tecnológicos que están asociados a los usuarios y contraseñas de acceso.

Con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis de los puntos de control que se citan dentro de los diferentes documentos del proceso, identificando controles específicos y con una periodicidad razonable para mitigar la materialización del riesgo.

Control 2

Se identifica que la evaluación del diseño del control, la información consignada en el aplicativo LUCHA arroja que tiene un responsable para ejecutar la actividad y se aplica cada vez que se requiere. Se encuentra documentado dentro de los lineamientos aportados desde el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 en sus capítulos 3.1 y 3.2 referidos a la administración del centro de cómputo y la aplicación del formato GT-FO-13 – REGISTRO DEL INGRESO AL CENTRO DE COMPUTO - V1 y se evidencia que no cuenta con observaciones o hallazgos de auditoria. Sin embargo, y con el ánimo de mejorar el blindaje sobre la ocurrencia del riesgo, se recomienda realizar un análisis sobre la periodicidad del control (Trimestral), ya que difiere de lo indicado por el proceso para el tratamiento del riesgo Caídas de Red que ejecuta este mismo control.

Se cuenta con rastros de ejecución del control para los primeros meses de la presente vigencia dada la situación de trabajo en casa.

Finalmente es importante manifestar que para todos los controles asociados a los riesgos del proceso (excepto el que tiene que ver con "Socializar Política"), se evidenció que para el manejo de desviaciones en la aplicación del control, se tomaron algunas medidas llevadas a cabo con relación a las condiciones de trabajo en casa desarrollado

en los últimos meses para la ejecución de los controles, las cuales se mencionaron en el acta de autoevaluación elaborada por el equipo de trabajo de gestión tecnológica; pero dichas medidas aún no se han documentado por lo cual no es posible evidenciarlas.

6.4. ANÁLISIS DEL PLAN DE CONTINGENCIA

Teniendo en cuenta que para el establecimiento de un plan de contingencia se deben identificar acciones que den pautas a seguir en caso de la materialización de los riesgos, el proceso de Gestión Tecnológica identificó las siguientes actividades, de las cuales se realizan las siguientes observaciones:

RIESGO	PLAN DE CONTINGENCIA ASOCIADO	OBSERVACIONES
1. Caídas de red (Comunicaciones, Internet, Sistemas)	**Actividad** Realizar mantenimientos a los equipos de comunicaciones, servidores y servicios. Actas de supervisión Diligenciar el formato de ingreso al centro de computo **Qué hacer antes** Backups de configuración para Routers, Switch y activos de red. Verificar el cumplimiento de las obligaciones del contrato **Qué hacer durante** Restauración de los servidores, bases de datos e información **Qué hacer después** Elaborar Plan de Mejoramiento	Las actividades identificadas como parte del plan de contingencia obedecen a controles ya establecidos para la mitigación del riesgo y son además actividades operativas que se deben realizar periódicamente, no se consideran como medidas adicionales; por ende, se recomienda analizar qué tipo de acciones o medidas adicionales podrían contribuir a la minimización del impacto en caso de materialización del riesgo y que en concordancia con la causa raíz del mismo se prioricen los posibles escenarios del riesgo identificando acciones reactivas. Se recomienda revisar que tipo de mantenimientos corresponderían a acciones para un plan de contingencia acorde con la minimización del impacto. En cuanto a las actividades del antes y durante una situación de materialización del riesgo, se observa que corresponden a medidas adicionales que se deben realizar para tratar de menguar las consecuencias del evento.
2. Pérdida de Información confidencial	**Actividad** Realizar backup de servidores e información crítica. Socializar la Política de Seguridad de la Información de la SDMujer. **Qué hacer antes** Backups de configuración para Routers, Switch y activos de red. Programación de campaña de concientización **Qué hacer durante** Restauración de los servidores, bases de datos e información **Qué hacer después** Elaborar Plan de Mejoramiento	En cuanto a la actividad referida a realizar backup de servidores e información crítica se considera parte del plan de contingencia, al igual que las acciones planteadas para el antes y el durante el evento en caso de materialización. En cuanto a la actividad relacionada con socializar la Política de Seguridad de la Información de la SDMujer, se recomienda analizar hasta qué punto podría ser parte de una contingencia para atacar el impacto de ocurrencia del riesgo o si se trata de una acción preventiva que beneficie la mitigación.
3. Eliminar y modificar información en las aplicaciones y bases de datos de la SDMujer.	**Actividad** Asignación de transporte para la mesa de ayuda Documentar el inventario de elementos requeridos para el soporte técnico **Qué hacer antes** Programar transporte permanente para el área de Gestión Tecnológica elaborar documento y solicitud de compra de partes **Qué hacer durante** Identificar las causas de la materialización del riesgo Identificar las causas de la materialización del riesgo **Qué hacer después** Elaborar Plan de Mejoramiento	No se evidencia relación coherente entre el riesgo formulado y la actividad y la acción que se establece para el Qué hacer antes, trazadas en el plan de contingencia, no se tratan de medidas adicionales para minimizar el impacto de la ocurrencia del evento. Se recomienda revisar que tipo de acciones corresponderían a un plan de contingencia que reduzcan las consecuencias referidas en el mapa de riesgos.

7. CONCLUSIONES

7.1. FORTALEZAS

En desarrollo del seguimiento se identificaron las siguientes fortalezas:

1. Se resalta el ejercicio de mejora continua llevado a cabo por el proceso "Gestión Tecnológica", relacionando la caracterización del proceso con la matriz de riesgos formulada.
2. De acuerdo con la autoevaluación realizada por el proceso de Gestión Tecnológica se evidencia que dicho ejercicio se llevó a cabo en el marco de los lineamientos dados institucionalmente, aplicando las preguntas orientadoras como parte del desarrollo de la mejora en la administración de sus riesgos.
3. También sobresale la identificación de situaciones coyunturales para la adecuada aplicación de los controles de los riesgos del proceso en cuanto a la cuarentena y el trabajo en casa a causa de la pandemia.

7.2. OPORTUNIDADES DE MEJORA

En desarrollo del presente seguimiento, se identificaron las siguientes oportunidades de mejora en cuanto a la administración del riesgo para el proceso "Gestión Tecnológica":

CUADRO DESCRIPTIVO OPORTUNIDADES DE MEJORA			
No	**DESCRIPCIÓN SITUACIÓN**	**Numeral del Informe**	**Responsable**
1.	Se recomienda articular la administración del riesgo del proceso "Gestión Tecnológica" con lo establecido en el Manual de Políticas Específicas de Seguridad de la Información con código GT-MA-3, sobre todo en lo que respecta al tratamiento de los riesgos ya que el manual indica que desde los dominios de seguridad de la información se establecen controles específicos para la mitigación de posibles eventos que afecten el cumplimiento del objetivo del proceso.	**6.1**	Proceso de Gestión Tecnológica
2.	Se recomienda realizar un análisis sobre la formulación de un riesgo relacionado con el atributo de privacidad de la información que se define dentro del habilitador transversal de seguridad de la información de la *Política de Gobierno Digital* establecida en el Modelo Integrado de Planeación y Gestión MIPG, con el fin de determinar si además del riesgo "*Perdida de información confidencial"* formulado por el proceso, podrían existir otros eventos que afectarían la privacidad de la información, no solo la que se considera según la ley como "*Confidencial"*.	**6.1**	Proceso de Gestión Tecnológica
3.	Se recomienda que el proceso realice el análisis de los niveles de aceptación y tratamiento de sus riesgos en concordancia con lo estipulado por la Política de Administración del Riesgo de la SDMujer Versión 3, en cuanto al establecimiento de controles, acciones preventivas y plan de contingencia según la zona del riesgo, de conformidad con la evaluación del riesgo inherente realizada por el proceso.	**6.1, 6.2 y 6.3**	Proceso de Gestión Tecnológica
4.	Nuevamente se indica la recomendación dada por este despacho en informes y seguimientos anteriores en relación con que los tiempos de aplicación de los controles para mitigar algunos de los riesgos son muy largos (según lo consignado en el módulo "riesgos y oportunidades" del aplicativo LUCHA), por lo que se recomienda identificar controles dentro de los documentos del proceso que se puedan ejecutar con mayor frecuencia y, así mismo, sea posible administrar los	**6.2 y 6.3**	Proceso de Gestión Tecnológica

CUADRO DESCRIPTIVO OPORTUNIDADES DE MEJORA			
No	**DESCRIPCIÓN SITUACIÓN**	**Numeral del Informe**	**Responsable**
	riesgos mediante puntos de control más específicos que realmente generen un grado de confiabilidad sobre la materialización.		
5.	Dado que no se evidenciaron rastros de aplicación de los controles para los riesgos 1 y 2, se recomienda determinar las evidencias que darán cuenta de su ejecución teniendo en cuenta los periodos definidos y los registros que se indican en los correspondientes procedimientos y/o manuales.	**6.2**	Proceso de Gestión Tecnológica
6.	Se recomienda que se realice la verificación correspondiente a los responsables de la ejecución de los controles identificados en la matriz de riesgos consignada en el aplicativo LUCHA, ya que se evidencia que en la mayoría de estos aparece la Jefa de la Oficina Asesora de Planeación como responsable de acciones operativas que no son congruentes con el manual de funciones para los diferentes cargos de la gestión tecnológica, ni tampoco con lo indicado por los procedimiento y manuales del proceso.	**6.2 y 6.3**	Proceso de Gestión Tecnológica
7.	Dado el ejercicio de mejora continua que realizó el proceso de Gestión Tecnológica recientemente, donde ajustó, actualizó y elaboró documentación pertinente para su operación, se recomienda articular la administración del riesgo con los lineamientos establecidos en el procedimiento GT-PR-13 - ADMINISTRACIÓN DEL PLAN DE CONTINUIDAD - V1, el cual en su actividad No. 2 indica que se debe analizar los impactos en el servicio y evaluar los riesgos correspondientes y en el procedimiento GT-PR-14 - GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - V1, que establece en la actividad No. 9 realizar el análisis de riesgos de la información.	**6**	Proceso de Gestión Tecnológica

7.3. HALLAZGOS

No se evidenciaron hallazgos.

	Tema o Palabras Clave	**Numeral del Informe**	**CONDICIÓN**	**CRITERIO**	**CAUSA**	**EFECTO**	**Proceso Responsable**	**ID LUCHA** (reincidencia)
1	N. A.	N. A.	N. A.	N. A.	N. A.	N. A.	N. A.	N. A.

Firma

(ORIGINAL FIRMADO)
Norha Carrasco Rincón
JEFA DE CONTROL INTERNO

	ANEXO 1. RIESGOS SDMUJER DICIEMBRE 2020																		
	ID LUCHA	Fecha identificación	Información General del Riesgo			DEBIDO A (CAUSA)	PUEDE OCURRIR (RIESGO ~ EVENTO)		LO QUE PODRÍA GENERAR (EFECTO ~ CONSECUENCIA)	1. Análisis del riesgo frente a la Caracterización del Proceso					2. Plan de Contingencia Revisar de acuerdo con Política de Riesgos		3. ANÁLISIS TRATAMIENTO ¿Esta acorde con la Política de Administración del Riesgo?	OBSERVACIONES OCI 1. Sobre relación Riesgo y Caracterización 2. Planes de Contingencia 3. Análisis de Tratamiento
			Categoría	Responsable	Procesos	Causas	Nombre del Riesgo	Descripción del Riesgo	Efectos	¿Las causas son coherentes con el riesgo ?	¿Las consecuencias son coherentes con las causas y el riesgo ?	¿Con cúales verbos clave del objetivo del proceso se relaciona?	¿El riesgo se relaciona con el objetivo del proceso?	¿La categoría del riesgo corresponde a la definición dada en la Guía Metodológica?	Plan de Contingencia	Avance Reporte Lucha Plan Contingencia En caso de materialización		
33	82	2017-02-03	- Riesgos tecnológicos (Riesgo tecnológico)	Adriana Estupiñan Jaramillo	- GESTION TECNOLOGICA	- 1. Daño de Equipos de comunicaciones. 2. Daño del Sistema de alimentación interrumpida (UPS). 3. El no pago de los servicios. 4. Errores humanos. (Origen: Interno | Factor: Recursos)	Caidas de red (Comunicaciones, Internet, Sistemas)	Caidas de red (Comunicaciones, Internet, Sistemas)	1. Retrasos y dificultadas en las labores de las servidoras y servidores de la Entidad. 2. Incumplimientos de las obligaciones de la entidad. 3. Perdida de información.	SI	SI	Planificar, gestionar, evaluar y optimizar la infraestructura tecnológica	SI	SI	Actividad Realizar mantenimientos a los equipos de comunicaciones, servidores y servicios. Actas de supervisión Diligenciar el formato de ingreso al centro de computo Qué hacer antes Backups de configuración para Routers, Switch y activos de red. Verificar el cumplimiento de las obligaciones del contrato Qué hacer durante Restauración de los servidores, bases de datos e información Qué hacer después Elaborar Plan de Mejoramiento	No se ha materializado el riesgo	NO faltan acciones preventivas	Se observa que la definición del riesgo corresponde con los verbos rectores del objetivo del proceso y se encuentra articulada con el ciclo PHVA de la caracterización, sobre todo para las actividades del HACER relacionadas con la gestión de seguridad de la información y la gestión de Soluciones y Servicios de Tecnología en cuanto a mantenimientos correctivos y preventivos y adicionalmente aplicando la metodología del metalenguaje se evidencia que la relación causa – riesgo – consecuencia se encuentra coherentemente relacionada. No se registra dentro del aplicativo LUCHA módulo de riesgos y oportunidades, rastros de la ejecución de los controles identificados para mitigar el riesgo; a pesar de que para el riesgo asociado a corrupción se contemplan los mismos controles y si se cuenta con los registros correspondientes a su aplicación. En cuanto al tratamiento del riesgo no se evidencia la aplicación de los lineamientos proferidos desde la Política de Administración del Riesgo SDMujer en su numeral 7, ya que para el tratamiento del presente riesgo, solo se formularon controles y plan de contingencia y por tratarse de un riesgo inherente en zona externa se debe formular adicionalmente acciones preventivas que ayuden a mitigar los efectos del riesgo. **PLAN DE CONTINGENCIA:** Se evidencia que se estableció como actividad "Realizar mantenimientos a los equipos...", lo que corresponde al control establecido para mitigar la ocurrencia del riesgo, en este sentido se recomienda analizar que tipo de acciones o medidas adicionales podrían contribuir a la minimización del impacto en caso de materializacion del riesgo y que en concordancia con la causa raíz del riesgo se prioricen los posibles escenarios del riesgo identificando acciones reactivas
34	83	2017-02-02	- Riesgos tecnológicos (Riesgo tecnológico)	Adriana Estupiñan Jaramillo	- GESTION TECNOLOGICA	- Caída de servidores (Origen: Interno | Factor: Recursos) - 1. Caidad de los servidores. 2. Manipulación de la información. 3. Falta de backup (respaldo externo). 4. Prestamo de usuarios y contraseñas. 5. Falta de seguridad Perimetral. (Origen: Sin definir | Factor: Sin definir) - 6. Accesos no autorizados al centro de computo. 7. Falta de seguridad fisica del centro de computo (acceso, aire, detectores de incedio, etc). 8. Daño fisico de discos duro (Servidores y Almacenamiento). 9. Segmentación de red servicios internos. (Origen: Sin definir | Factor: Sin definir)	Perdida de Información confidencial	Perdida de Información confidencial	1. Retrasos y dificultadas en las labores de las servidoras y servidores de la Entidad. 2. Reportes erroneos. 1. Duplicidad de la información. 2. Bajos niveles de seguridad en la información. 3. Retrasos en el procesamiento de datos por la necesidad de verificar y depurar la información.	SI	SI	Velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información	SI	SI	Actividad Realizar backup de servidores e información crítica Socializar la Política de Seguridad de la Información de la SDMujer. Qué hacer antes Backups de configuracion para Routers, Switch y activos de red. Programación de campaña de concientización Qué hacer durante Restauración de los servidores, bases de datos e información Qué hacer después Elaborar Plan de Mejoramiento	No se ha materializado el riesgo	NO faltan acciones preventivas	En revisión de la coherencia entre los elementos de la caracterización del proceso y el riesgo formulado, se evidencia que el objetivo esta asociado con las actividades clave sobre todo en lo concerniente con velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información. Adicionalmente esta el riesgo se articula con las actividades descritas en el ciclo PHVA , toda vez que la materialización del evento puede afectar negativamente el cumplimiento del objetivo del proceso. Aplicando la metodología del metalenguaje se evidencia que la relación causa – riesgo – consecuencia es coherente. No se registra dentro del aplicativo LUCHA módulo de riesgos y oportunidades, rastros de la ejecución de los controles identificados para mitigar el riesgo; a pesar de que para el riesgo asociado a corrupción se contemplan los mismos controles y si se cuenta con los registros correspondientes a su aplicación. Por otra parte se observa que el riesgo no tiene en cuenta lo establecido desde la Política de Administración del Riesgo ya que para el tratamiento solo se formularon controles y plan de contingencia y por tratarse de un riesgo inherente en zona externa se debe formular adicionalmente acciones preventivas que ayuden a mitigar los efectos del riesgo. **PLAN DE CONTINGENCIA:** En cuanto a la actividad referida a realizar backup de servidores e información crítica se considera parte del plan de contingencia, al igual que las acciones planteadas para el antes y el durante el evento en caso de materialización. En cuanto a la actividad relacionada con socializar la Política de Seguridad de la Información de la SDMujer, se recomienda analizar hasta qué punto podría ser parte de una contingencia para atacar el impacto de ocurrencia del riesgo o si se trata de una acción preventiva que beneficie la mitigación.
35	86	2017-02-03	- Riesgos tecnológicos (Riesgo tecnológico)	Adriana Estupiñan Jaramillo	- GESTION TECNOLOGICA	- 1. Falta de herramientas para el control de la seguridad de la información. 2. Falta de actualización de credenciales de usuarios de los diferentes aplicativos y sistemas de información. 3. Prestamo de la clave de acceso. (Origen: Externo | Factor: Tecnológico)	Eliminar y modificar información en las aplicaciones y bases de datos de la SDMujer.	Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad.	Impide la ejecución exitosa de otros procesos y afecta la competitividad de la entidad. Incide en la calidad de la información, en la agilidad, costos y credibilidad en cuanto a los procedimientos y seguridad de los mismos.	SI	SI	Velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información	SI	SI	Actividad Realizar mantenimientos a los equipos de comunicaciones, servidores y servicios. Actas de supervisión Diligenciar el formato de ingreso al centro de computo Qué hacer antes Backups de configuración para Routers, Switch y activos de red. Verificar el cumplimiento de las obligaciones del contrato Qué hacer durante Restauración de los servidores, bases de datos e información Qué hacer después Elaborar Plan de Mejoramiento	No se ha materializado el riesgo	NO faltan acciones preventivas	En cuanto al riesgo identificado se observa que este se relaciona con el verbo del objetivo que tiene que ver con velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información. Dentro del ciclo PHVA del proceso se visualizan acciones concernientes como gestionar tanto la Seguridad de la Información y soluciones y servicios de tecnología, por lo cual existen procedimientos relacionados. Para la relación entre causa-riesgo y consecuencia se observa que se guarda la coherencia de acuerdo con la metodología del metalenguaje. Igualmente que los riesgos anteriores, el riesgo evaluado no contempla lo establecido en el numeral 7 de la Política de Administración del Riesgo ya que para el tratamiento se formularon controles y plan de contingencia y por tratarse de un riesgo inherente en zona alta se debe formular controles y acciones preventivas que ayuden a disminuir las consecuencias en caso de materialización del riesgo. **PLAN DE CONTINGENCIA: No se evidencia relación coherente entre el riesgo formulado y la actividad y la acción del antes, trazadas en el plan de contingencia, no se tratan de medidas adicionales para minimizar el impacto de la ocurrencia del evento. Se recomienda revisar que tipo de acciones corresponderían a un plan de contingencia que reduzcan las consecuencias referidas en el mapa de riesgos.**

ANEXO 1. RIESGOS SDMUJER DICIEMBRE 2020																		
ID LUCHA	**Fecha identificación**	**Información General del Riesgo**			**DEBIDO A (CAUSA)**	**PUEDE OCURRIR (RIESGO ~ EVENTO)**		**LO QUE PODRÍA GENERAR (EFECTO ~ CONSECUENCIA)**	**1. Análisis del riesgo frente a la Caracterización del Proceso**					**2. Plan de Contingencia Revisar de acuerdo con Política de Riesgos**		**3. ANÁLISIS TRATAMIENTO ¿Esta acorde con la Política de Administración del Riesgo?**	**OBSERVACIONES OCI 1. Sobre relación Riesgo y Caracterización 2. Planes de Contingencia 3. Análisis de Tratamiento**
		Categoría	**Responsable**	**Procesos**	**Causas**	**Nombre del Riesgo**	**Descripción del Riesgo**	**Efectos**	**¿Las causas son coherentes con el riesgo ?**	**¿Las consecuencias son coherentes con las causas y el riesgo ?**	**¿Con cúales verbos clave del objetivo del proceso se relaciona?**	**¿El riesgo se relaciona con el objetivo del proceso?**	**¿La categoría del riesgo corresponde a la definición dada en la Guía Metodológica?**	**Plan de Contingencia**	**Avance Reporte Lucha Plan Contingencia En caso de materialización**		
45	115	2019-01-25	- Riesgos asociados a corrupción (Riesgos asociados a corrupción)	Adriana Estupiñan Jaramillo	- GESTION TECNOLOGICA	- Debilidades en la implementación de controles de acceso. (Origen: Interno | Factor: Recursos) - Intereses particulares de servidoras(es) públicos y/o contratistas (Origen: Interno | Factor: Cultura) - Presiones indebidas u ofrecimiento de dádivas por parte de terceros (Origen: Interno | Factor: Cultura)	Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad	Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad	Retrasos y dificultadas en las actividades operativas y misionales de la Entidad. Manipulación indebida de la información Imposibilidad de recurerar la información Alteración y/o venta de los datos e información de la Entidad y de Terceros en beneficio propio o de un tercero	SI	SI	Garantizar la seguridad y la continuidad de la infraestructura tecnológica y velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información	SI	SI	No se formulo el plan de contigencia correspondiente	No se ha materializado el riesgo	NO falta el plan de contingencia	Se evidencia que este evento se relaciona con los verbos rectores del objetivo del proceso en cuanto a garantizar la seguridad y la continuidad de la infraestructura tecnológica y asimismo velar por la confidencialidad, integridad, disponibilidad y autenticidad de la información; identificándose actividades concretas dentro del ciclo PHVA del proceso y sus procedimientos correspondientes. Por otra parte se observa que para el tratamiento del riesgo asociado a corrupción no se ha tenido en cuenta lo establecido desde la Política de Administración del Riesgo en cuanto a los niveles de aceptación y tratamiento, dado que por tratarse de un riesgo inherente en zona extrema se deben formular controles, plan de contigencia y acciones preventivas que ayuden a mitigar los efectos del riesgo. **PLAN DE TRATAMIENTO: -** Seguimiento a la ejecución del cronograma de mantenimientos - Seguimiento a la ejecución de los Backup en la periodicidad establecida en la política de backup de la Entidad - Socializar la Política de Seguridad de la Información de la SDMujer.

ANEXO 2. MATRIZ DE CONTROLES DE RIESGOS SDMUJER

No.	RIESGOS			CONTROLES								EVALUACIÓN DEL DISEÑO DE CONTROLES									EVALUACIÓN DE LA EJECUCIÓN DEL CONTROL - EVIDENCIAS LUCHA			SOLIDEZ DEL CONTROL		OBSERVACIONES FINALES OCI
	ID LUCHA	Fecha identificación	Nombre	ID	Nombre	Control	Periodicidad de ejecución	Tipo de control	Tipo de manejo	Naturaleza del control	Responsable de ejecución	Responsable	¿Responsable con autoridad y adecuada segregación de funciones?	Periodicidad	Propósito	¿Manejo de desviaciones?	¿Evidencia o rastro de la ejecución?	¿Formalizado en documentos del Proceso (LUCHA)?	TOTAL EVALUACIÓN DISEÑO		Ejecucion del control	Materialización y/o Hallazgos	EVALUACIÓN EJECUCIÓN	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	
																			Puntaje	Clasificación						
33	82	2017-02-03	Caidas de red (Comunicaciones, Internet, Sistemas)	163	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Anual	Preventivo	Reducir	Manual	- Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Inoportuna	Prevenir	Incompleto	Incompleta	SI	67	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL	DEBIL	En revisión del control se observa que su diseño es fuerte dado que está documentado dentro del instructivo nombradoMANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3, especificando los responsables de llevarlo a cabo y para algunas actividades se identifica su periodicidad. Sin embargo, para su ejecución se califica como moderada para mitigar el riesgo asociado, ya que la aplicación del control es una actividad que requiere de un plan de trabajo compuesto por varias acciones puntuales para desarrollarlo, lo cual podría tornar el control en una herramienta difícil de manejar ya que necesita varios responsables para su aplicación y las diferentes acciones tienen una periodicidad variada. Adicionalmente y con base en lo reportado dentro del aplicativo LUCHA módulo de riesgos, se retoman algunas observaciones dadas en seguimientos anteriores ya que se evidencia que a pesar de que el control se utiliza y no cuenta con observaciones o hallazgos de auditoria, no es pertinente identificar un control que solo se pueda ejecutar cada año, esto dado que el riesgo Caídas de red involucra un impacto muy alto sobre la gestión propia de la entidad, con unas consecuencias que podrían estar relacionadas con parar la operación de la entidad. Por estas razones se recomienda analizar la pertinencia del control por parte del proceso de gestión tecnológica, teniendo en cuenta los documentos MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 y GT-PR-16 - GESTIÓN DE SOLUCIONES Y SERVICIOS - V1 en lo que respecta a mantenimientos preventivos y correctivos tamto de hardware como de sotfware, identificando los puntos de control como controles individuales, reconocidos por los responsables de aplicarlos y con una periodicidad razonable para mitigar la materialización del riesgo. Para el manejo de desviaciones en la aplicación del control, se evidencio a través del acta de autoevaluación elaborada por el equipo de trabajo de gestión tecnológica se mencionó que se tomaron algunas medidas relacionadas con la ejecución de los controles, dadas las condiciones de trabajo en casa, pero dichas medidas aún no se han documentado por lo cual no es posible evidenciarlas.
				165	Establecer control de acceso al centro de cómputo	Establecer control de acceso al centro de cómputo	Cuando se requiera	Preventivo	Reducir	Manual	- ANDRES CAMACHO NIETO - Miguel Alberto Bernal Garnica - Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Oportuna	Prevenir	Incompleto	Incompleta	SI	82	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL		Se identifica que la evaluación del diseño del control, la información consignada en el aplicativo LUCHA arroja que tiene un responsable para ejecutar la actividad y se aplica cada vez que se requiere. Se encuentra documentado dentro de los lineamientos aportados desde el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 en sus capítulos 3.1 y 3.2 referidos a la administración del centro de cómputo y la aplicación del formato GT-FO-13 – REGISTRO DEL INGRESO AL CENTRO DE COMPUTO - V1 y se evidencia que no cuenta con observaciones o hallazgos de auditoria. No se cuenta con rastros de ejecución del control, pero es importante acotar que en revisión de la herramienta LUCHA, se observó que el control se aplica también en el riesgo asociado a corrupción y desde allí si se indica la evidencia relacionada para los primeros meses de la presente vigencia dada la situación de trabajo en casa; evidencia que fue consignada y reportada dentro del módulo. Al igual que el control anterior, para el manejo de desviaciones en la aplicación del control, se evidencio que a través del acta de autoevaluación elaborada por el equipo de trabajo de gestión tecnológica se mencionó que se tomaron algunas medidas relacionadas con la ejecución de los controles, dadas las condiciones de trabajo en casa, pero dichas medidas aún no se han documentado por lo cual no es posible evidenciarlas.
34	83	2017-02-02	Perdida de Información confidencial	166	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Anual	Preventivo	Reducir	Manual	- Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Inoportuna	Prevenir	Incompleto	Incompleta	SI	67	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL	DEBIL	En revisión del control se observa que su diseño es fuerte dado que está documentado dentro del instructivo nombradoMANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3, especificando los responsables de llevarlo a cabo y para algunas actividades se identifica su periodicidad. Sin embargo, para su ejecución se califica como moderada para mitigar el riesgo asociado, ya que la aplicación del control es una actividad que requiere de un plan de trabajo compuesto por varias acciones puntuales para desarrollarlo, lo cual podría tornar el control en una herramienta difícil de manejar ya que necesita varios responsables para su aplicación y las diferentes acciones tienen una periodicidad variada. Adicionalmente y con base en lo reportado dentro del aplicativo LUCHA módulo de riesgos, se retoman algunas observaciones dadas en seguimientos anteriores ya que se evidencia que a pesar de que el control se utiliza y no cuenta con observaciones o hallazgos de auditoria, no es pertinente identificar un control que solo se pueda ejecutar cada año, esto dado que el riesgo Caídas de red involucra un impacto muy alto sobre la gestión propia de la entidad, con unas consecuencias que podrían estar relacionadas con parar la operación de la entidad. Por estas razones se recomienda analizar la pertinencia del control por parte del proceso de gestión tecnológica, teniendo en cuenta los documentos MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 y GT-PR-16 - GESTIÓN DE SOLUCIONES Y SERVICIOS - V1 en lo que respecta a mantenimientos preventivos y correctivos tamto de hardware como de sotfware, identificando los puntos de control como controles individuales, reconocidos por los responsables de aplicarlos y con una periodicidad razonable para mitigar la materialización del riesgo. Para el manejo de desviaciones en la aplicación del control, se evidencio a través del acta de autoevaluación elaborada por el equipo de trabajo de gestión tecnológica se mencionó que se tomaron algunas medidas relacionadas con la ejecución de los controles, dadas las condiciones de trabajo en casa, pero dichas medidas aún no se han documentado por lo cual no es posible evidenciarlas.
				167	Realizar Backup de servidores, aplicaciones y configuraciones según politica de backup para la SDMujer	Realizar Backup de servidores, aplicaciones y configuraciones según politica de backup para la SDMujer	Mensual	Preventivo	Reducir	Combinado	- Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Inoportuna	Prevenir	Definido	Incompleta	SI	77	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL		El control se encuentra documentado como parte de los protocolos establecidos en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 que en su aparte 3.10 Administración de Backup y recuperación de la información, indica la política de operación para backup de los sistemas operativos, bases de datos, aplicaciones y recursos compartidos. Asimismo, se identifican los responsables de realizar los correspondientes respaldos de información y verificación de acuerdo con el tipo de elemento o recurso de almacenamiento. No se evidencian observaciones o hallazgos de auditoria relacionados con la aplicación del control y se cuenta con el registro de la evidencia relacionada para los primeros meses de la vigencia dada la situación de trabajo en casa. En lo relacionado con el periodo de ejecución del control, el manual indica diferentes momentos en el tiempo para realizar el backup para los sistemas operativos, bases de datos, aplicaciones y recursos compartidos; lo cual difiere con lo consignado en la matriz de riesgos ya que allí se señala que esta actividad se debe llevar a cabo mensualmente. Se recomienda revisar la pertinencia del periodo de ejecución que se establece, ya que esto podría generar confusiones al momento de la aplicación del control por parte de los responsables; es así que se hace necesario analizar si se requiere ampliar el control mencionado las especificidades para los recursos de almacenamiento (sistemas operativos, bases de datos, aplicaciones y recursos compartidos). El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado, pero dado que el documento fue implememntado reciente mente no se evidencian registros sobre el particular.

ANEXO 2. MATRIZ DE CONTROLES DE RIESGOS SDMUJER

No.	RIESGOS			CONTROLES								EVALUACIÓN DEL DISEÑO DE CONTROLES									EVALUACIÓN DE LA EJECUCIÓN DEL CONTROL - EVIDENCIAS LUCHA			SOLIDEZ DEL CONTROL		OBSERVACIONES FINALES OCI
	ID LUCHA	Fecha identificación	Nombre	ID	Nombre	Control	Periodicidad de ejecución	Tipo de control	Tipo de manejo	Naturaleza del control	Responsable de ejecución	Responsable	¿Responsable con autoridad y adecuada segregación de funciones?	Periodicidad	Propósito	¿Manejo de desviaciones?	¿Evidencia o rastro de la ejecución?	¿Formalizado en documentos del Proceso (LUCHA)?	TOTAL EVALUACIÓN DISEÑO		Ejecucion del control	Materialización y/o Hallazgos	EVALUACIÓN EJECUCIÓN	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	
																			Puntaje	Clasificación						
				168	Socializar la política de seguridad de la SDMujer	Socializar la política de seguridad de la SDMujer	Anual	Preventivo	Reducir	Manual	- Adriana EstupiÃ±an Jaramillo				No es un control				0	DEBIL			DEBIL	DEBIL		Se retoma la observación aportada por este despacho en varios informes y seguimientos, en cuanto a las actividades relacionadas con socializar o dar a conocer cualquier tipo de documento o información, ya que esta no corresponde a un control. Para esta acción en específico Socializar la política de seguridad de la SDMujer se observa que no es posible controlar o determinar qué tanto del tema socializado quedó interiorizado en los participantes y adicionalmente se le asigna una periodicidad muy larga para su aplicación que se podría generar un impacto significativo en caso de materialización del riesgo. Es por esto que se recomienda formular controles de carácter permanente y acordes al volumen de información que se produce continuamente en la entidad. Para este tipo de actividades que se relacionan con talleres, socializaciones o capacitaciones sobre temas específicos o para dar a conocer normas o documentos a implementar, se recomienda analizar la posibilidad de identificarlas como acción preventiva para reforzar el tratamiento del riesgo.
				248	Monitorear las amenazas que puedan vulnerar los equipos de cómputo, así como la información de la entidad	Monitorear las amenazas que puedan vulnerar los equipos de cómputo, así como la información de la entidad	Mensual	Preventivo	Reducir	Manual	- Adriana EstupiÃ±an Jaramillo	Asignado	Inadecuado	Inoportuna	Prevenir	No definido	No Existe	NO	30	DEBIL	El control no se ejecuta por parte del responsable	NO	DEBIL	DEBIL		En revisión de los documentos del proceso, se identificó que la actividad indicada como control no se enuncia específicamente sobre la operación del proceso; se evidenció que dentro de los protocolos determinados en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 se contempla la gestión de incidentes de seguridad de la información de acuerdo con el tipo de incidente que llegara a presentarse y en este sentido se clasifican también el nivel de criticidad y de escalonamiento con que debe tratarse y los responsables en cada caso. Es así que a pesar de que el control formulado no se encuentra textualmente enunciado en los documentos del proceso, se percibe que podría estar asociado con lo establecido por los lineamientos del manual de gestión tecnológica; por lo que se recomienda analizar si se requiere indicar específicamente la realización de este tipo de monitoreos y además evidenciar la periodicidad con que se requiere aplicar el control, máxime que dichos lineamientos declaran la utilización de un formato de registro de incidentes de seguridad de la información que no se encuentra formalizado en el aplicativo LUCHA.
35	86	2017-02-03	Eliminar y modificar información en las bases de datos de los sistemas de información de la entidad.	175	Programar el cambio de contraseña de los usuarios cada 45 días	Programar el cambio de contraseña de los usuarios cada 45 días	Mensual	Correctivo	Reducir	Combinado	- Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Oportuna	Prevenir	Definido	Completa	SI	100	FUERTE	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	FUERTE	MODERADO	La actividad identificada como control se encuentra documentada en los lineamientos aportados desde el MANUAL DE LINEAMIENTOS HERRAMIENTAS TECNOLOGICAS GT-MA-2 en su versión 1, por lo que cumple con los criterios que se designan para el diseño y se evidencia que se ejecuta de manera consistente por parte del responsable; por otro lado, no se tienen hallazgos de auditoria asociados y el riesgo no se ha materializado durante el lapso de su seguimiento actual. Se recomienda articular la periodicidad establecida en el aplicativo LUCHA (mensual) con la periodicidad descrita en el control (45 días) y asimismo con la aplicación de este mismo para el riesgo asociado a corrupción. El proceso indica que para este periodo de evaluación y debido a la contingencia por la emergencia sanitaria, se amplió el tiempo de definido de cambio de contraseñas, con el fin de minimizar el impacto de negación de acceso a los servicios tecnológicos que están asociados a los usuarios y contraseñas de acceso. El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado. Con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis de los puntos de control que se citan dentro de los diferentes documentos del proceso, identificando controles específicos y con una periodicidad razonable para mitigar la materialización del riesgo.
				176	Realizar Backup de servidores, aplicaciones y configuraciones según politica de backup para la SDMujer	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	Mensual	Preventivo	Reducir	Manual	- Adriana EstupiÃ±an Jaramillo	Asignado	Adecuado	Inoportuna	Prevenir	Definido	Completa	SI	85	DEBIL	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	DEBIL		El control se encuentra documentado como parte de los protocolos establecidos en el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 que en su aparte 3.10 Administración de Backup y recuperación de la información, indica la política de operación para backup de los sistemas operativos, bases de datos, aplicaciones y recursos compartidos. Asimismo, se identifican los responsables de realizar los correspondientes respaldos de información y verificación de acuerdo con el tipo de elemento o recurso de almacenamiento. No se evidencian observaciones o hallazgos de auditoria relacionados con la aplicación del control. En lo relacionado con el periodo de ejecución del control, el manual indica diferentes momentos en el tiempo para realizar el backup para los sistemas operativos, bases de datos, aplicaciones y recursos compartidos; lo cual difiere con lo consignado en la matriz de riesgos ya que allí se señala que esta actividad se debe llevar a cabo mensualmente. Se recomienda revisar la pertinencia del periodo de ejecución que se establece, ya que esto podría generar confusiones al momento de la aplicación del control por parte de los responsables; es así que se hace necesario analizar si se requiere ampliar el control mencionado las especificidades para los recursos de almacenamiento (sistemas operativos, bases de datos, aplicaciones y recursos compartidos). El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado, pero dado que el documento fue implememntado reciente mente no se evidencian registros sobre el particular. Para este riesgo en particular no se cuenta con registros de su ejecución dentro del módulo de riesgos y oportunidades del aplicativo LUCHA, no obstante, en revisión de la herramienta se observó que el presente control también se aplica para el riesgo 3 y desde allí si se cuenta con la evidencia relacionada para los primeros meses de la vigencia dada la situación de trabajo en casa, evidencia que fue consignada y reportada dentro de dicho módulo.
45	115	2019-01-25	Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad	274	Programar el cambio de contraseña de los usuarios cada 45 días	Programar el cambio de contraseña de los usuarios cada 45 días	Trimestral	Preventivo	Reducir		- ANDRES CADENA HERRERA	Asignado	Adecuado	Inoportuna	Prevenir	Definido	Completa	SI	85	DEBIL	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	DEBIL	DEBIL	La actividad identificada como control se encuentra documentada en los lineamientos aportados desde el MANUAL DE LINEAMIENTOS HERRAMIENTAS TECNOLOGICAS GT-MA-2 en su versión 1, por lo que cumple con los criterios que se designan para el diseño y se evidencia que se ejecuta de manera consistente por parte del responsable; por otro lado, no se tienen hallazgos de auditoria asociados y el riesgo no se ha materializado durante el lapso de su seguimiento actual. Se recomienda articular la periodicidad establecida en el aplicativo LUCHA (trimestral) con la periodicidad descrita en el control y con la aplicación de este mismo para el riesgo relacionado con eliminar y modificar información en las bases de datos de los sistemas de información de la entidad. El proceso indica que para este periodo de evaluación y debido a la contingencia por la emergencia sanitaria, se amplió el tiempo de definido de cambio de contraseñas, con el fin de minimizar el impacto de negación de acceso a los servicios tecnológicos que están asociados a los usuarios y contraseñas de acceso. El manejo de desviaciones sobre la ejecución del control se encuentra enunciado en el manual mencionado. Con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis de los puntos de control que se citan dentro de los diferentes documentos del proceso, identificando controles específicos y con una periodicidad razonable para mitigar la materialización del riesgo.

ANEXO 2. MATRIZ DE CONTROLES DE RIESGOS SDMUJER

No.	RIESGOS			CONTROLES								EVALUACIÓN DEL DISEÑO DE CONTROLES									EVALUACIÓN DE LA EJECUCIÓN DEL CONTROL - EVIDENCIAS LUCHA			SOLIDEZ DEL CONTROL		OBSERVACIONES FINALES OCI
	ID LUCHA	Fecha identificación	Nombre	ID	Nombre	Control	Periodicidad de ejecución	Tipo de control	Tipo de manejo	Naturaleza del control	Responsable de ejecución	Responsable	¿Responsable con autoridad y adecuada segregación de funciones?	Periodicidad	Propósito	¿Manejo de desviaciones?	¿Evidencia o rastro de la ejecución?	¿Formalizado en documentos del Proceso (LUCHA)?	TOTAL EVALUACIÓN DISEÑO		Ejecucion del control	Materialización y/o Hallazgos	EVALUACIÓN EJECUCIÓN	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	
																			Puntaje	Clasificación						
			Eliado	275	Establecer control de acceso al centro de cómputo	Establecer control de acceso al centro de cómputo	Trimestral	Preventivo	Reducir		- ANDRES CADENA HERRERA	Asignado	Adecuado	Inoportuna	Prevenir	Incompleto	Completa	SI	75	DEBIL	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	DEBIL		Se identifica que la evaluación del diseño del control, la información consignada en el aplicativo LUCHA arroja que tiene un responsable para ejecutar la actividad y se aplica cada vez que se requiere. Se encuentra documentado dentro de los lineamientos aportados desde el MANUAL GESTIÓN TECNOLÓGICA - GT-MA-1 - V3 en sus capítulos 3.1 y 3.2 referidos a la administración del centro de cómputo y la aplicación del formato GT-FO-13 – REGISTRO DEL INGRESO AL CENTRO DE COMPUTO - V1 y se evidencia que no cuenta con observaciones o hallazgos de auditoria. Sin embargo, y con el ánimo de mejorar el blindaje sobre la ocurrencia del riesgo, se recomienda realizar un análisis sobre la periodicidad del control (Timestral), ya que difiere de lo indicado por el proceso para el tratamiento del riesgo Caídas de Red que ejecuta este mismo control. Se cuenta con rastros de ejecución del control para los primeros meses de la presente vigencia dada la situación de trabajo en casa. Al igual que el control anterior, para el manejo de desviaciones en la aplicación del control, se evidencio que a través del acta de autoevaluación elaborada por el equipo de trabajo de gestión tecnológica se mencionó que se tomaron algunas medidas relacionadas con la ejecución de los controles, dadas las condiciones de trabajo en casa, pero dichas medidas aún no se han documentado por lo cual no es posible evidenciarlas.