INFORME DE SEGUIMIENTO

GESTIÓN DEL RIESGO DE LA SECRETARÍA DISTRITAL DE LA MUJER

PROCESO GESTIÓN TECNOLOGÍCA

OFICINA DE CONTROL INTERNO

Norha Carrasco Rincón
JEFA DE LA OFICINA DE CONTROL INTERNO

EQUIPO AUDITOR
Diana Carolina Henao Rosas – Técnica Administrativa
Yazmín Alexandra Beltrán Rodríguez – Contratista
Claudia Patricia Morales Morales – Contratista
Claudia Cuesta Hernández – Profesional Especializado

PERIODO EVALUADO
Enero – Noviembre 2019

FECHA DEL INFORME
Diciembre de 2019

Contenido

1. OBJETIVOS DEL SEGUIMIENTO

Realizar el seguimiento a la gestión del riesgo llevada a cabo por los procesos de acuerdo con las orientaciones dadas desde 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).

2. 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 2019.

3. 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 2 de diciembre de 2018).

4. RESULTADOS Y EVIDENCIAS RELACIONADAS

4.1. 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 4.1.1, 4.1.2 y 4.1.3 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.

4.1.1. 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, n 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 1. 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.

4.1.2. Idoneidad del diseño de controles

Para identificar si las características de los controles asociados a los riesgos reúnen o cumplen con 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 para lo cual se utilizan los siguientes:

- Responsabilidad
- Periodicidad
- Propósito
- Actividad del Control
- Ejecución del Control

Tabla 2. 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
		18		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	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable		No confiable
		15		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	7	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 3.

Tabla 3. 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 3, 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.

[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.

4.1.3. 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 4 se resume la forma de realizar esta calificación, y la conclusión asociada a cada tema.

Tabla 4. 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 halazgos 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 4, 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.

4.1.4. 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 5.

Tabla 5. 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.

4.2. ANÁLISIS DE RIESGOS DE GESTIÓN DEL PROCESO GESTIÓN TECNOLOGÍCA

Los riesgos de gestión asociados al proceso "Gestión Tecnológica" se presentan en la Tabla 6.

Tabla 6. Riesgos de gestión del proceso "Gestión Tecnológica"
Estructura del riesgo

Objetivo del proceso: Proveer, gestionar, facilitar, desarrollar e implementar una estrategia de recursos tecnológicos, que permita poner a disposición de toda la SDMujer, una infraestructura tecnológica basada en herramientas informáticas, servicios de redes y comunicaciones que contribuyan a elevar la eficiencia y la efectividad en el cumplimiento de la misión.

	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*	**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.
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*	**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*	**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 4.1 del presente informe, en relación con la estructura de los riesgos identificados se puede concluir lo siguiente:

1. Aplicando la metodología del metalenguaje se evidencia que la relación causa – riesgo – consecuencia es coherente y consistente con la estructura de los riesgos formulados.

2. Las tipologías de los riesgos son coherentes con las consecuencias de la materialización de los riesgos y la temática de que trata el proceso de gestión tecnológica.

3. De acuerdo con el seguimiento realizado, se recomienda revisar el contexto de identificación de los riesgos del proceso teniendo en cuenta el objetivo, el alcance y el ciclo PHVA del proceso de Gestión Tecnológica, de modo que se visibilice el desarrollo y la implementación de la estrategia de recursos tecnológicos de que trata el objetivo; esto con el fin de fortalecer la coherencia que debe existir entre la caracterización del proceso y los riesgos identificados.

4. En el marco de la *Política de Seguridad de la Información de la SDMujer* formalizada recientemente, se observa que en el aparte de aplicabilidad se identifican la información, el software y el hardware como elementos pasa su operación y administración, 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. Además, seria importante realizar la articulación correspondiente del mapa de riesgos con que se cuenta hasta la fecha, con todos los lineamientos establecidos por dicha política, para fortalecer la administración de este tipo de riesgos en la entidad.

5. Por otra parte, se recomienda que en el marco de la implementación de la P*olítica de Gobierno Digital (Manual Técnico MIPG)*, 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"*.

Teniendo en cuenta lo anterior, se procedió a analizar los controles identificados para prevenir la materialización del riesgo o para mitigar sus consecuencias.

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

Este riesgo cuenta con dos controles a los que se realizó la evaluación de diseño y ejecución (Anexo 1), dando como resultado que el conjunto de controles tiene una solidez débil, como se resume en la Tabla 7 (el detalle se encuentra en el Anexo 1).

Tabla 7. 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.	**100**: Fuerte	Moderado	Moderado	Débil
2	Establecer control de acceso al centro de cómputo	**67**: Débil	Moderado	Débil	

A continuación, se relaciona el análisis realizado para cada control:

Control No. 1

De acuerdo con lo observado, el diseño del control es fuerte dado que está documentado dentro del instructivo nombrado *Plan de Mantenimiento Preventivo a Equipos Informáticos con código GT-PL-01*, 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 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 y actualizar el instructivo nombrado *"Plan de Mantenimiento Preventivo a Equipos Informáticos"*, 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.

Control No. 2

El control *"Establecer control de acceso al centro de cómputo"*, cumple con los criterios de diseño en cuanto a su documentación en el aplicativo LUCHA y cuenta con un responsable de su aplicación. No obstante, no se evidencia la segregación de funciones en la aplicación del control. Para la evidencia de su aplicación se encontró que a través del *Manual de Gestión Tecnológica* con código GT-MA-01 y el uso de los formatos *GT-FO-13 – Registro del Ingreso al Centro de Computo - V1 y GT-FO-14 - Solicitud de Acceso al Centro de Computo - V1* se mitiga el riesgo. Sin embargo, y con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis en primera instancia sobre la periodicidad del control (Semestral) y de los puntos de control que se citan dentro del manual, identificando controles específicos y con una periodicidad razonable; esto dado que los riesgos de tipo tecnológico generalmente requieren ser controlados casi que diariamente.

Realizando la evaluación correspondiente de los controles identificados para el riesgo *Caídas de Red*, se observa que tienen una periodicidad muy larga para su aplicación (semestral y anual), lo cual implica que puede existir una brecha para la materialización del riesgo, dado que el impacto de ocurrencia puede llegar a ser ALTO para la gestión propia de la entidad y adicionalmente puede desencadenar en que se materialicen otros riesgos como el de perdida de la información. Por esta razón se recomienda analizar la pertinencia de los controles formulados por parte del proceso de gestión tecnológica.

4.2.2. Análisis de controles del riesgo "Perdida de Información confidencial".

Este riesgo cuenta con cinco controles a los que se realizó la evaluación de diseño y ejecución (Anexo 1), dando como resultado que el conjunto de controles tiene una solidez débil, como se resume en la Tabla 8 (el detalle se encuentra en el Anexo 1).

Tabla 8. 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.	**100**: Fuerte	Moderado	Moderado	Débil
2	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	**85**: Débil	Fuerte	Débil	
3	Socializar la política de seguridad de la SDMujer	No es un Control	N. A.	N. A.	
4	Documentar el ciclo de vida de los desarrollos de software, in house y/o contratados.	40: Débil	Débil	Débil	
5	Escanear vulnerabilidades a la infraestructura de TI	35: Débil	Débil	Débil	

A continuación, se relaciona el análisis realizado para cada control:

Control 1

Se retoma lo observado en el riesgo anterior, en cuanto a que el control es evaluado como débil ya que se encontró que, al tener periodos de aplicación tan largos, la pérdida de información se puede materializar en cualquier momento, a pesar de estar formalizado en el instructivo Plan de Mantenimiento Preventivo a Equipos Informáticos GT-PL-01.

Control 2

El control relacionado se encuentra documentado dentro del procedimiento *GT-PR-4 Administración de Backups y Restauración de la Información*, que para la aplicación de sus actividades se observa una inadecuada segregación de funciones dado que no se evidencia un responsable con autoridad para avalar el cumplimiento de los lineamientos para realizar los respectivos backups. Por otra parte, y en cuanto a la periodicidad de su ejecución para el riesgo en evaluación, se evidencia que al tener periodos de aplicación del control tan largos (Anual), la perdida de información se puede materializar en cualquier momento

En cuanto a la normatividad que enuncia el procedimiento *GT-PR-4 Administración de Backups y Restauración de la Información*, se recomienda actualizar los documentos que allí se relacionan, ya que se identifica un *Protocolo de Administración de Backup código GT-IN-1* que ya no se encuentra dentro del listado de documentos del proceso de gestión tecnológica ni aparece en el módulo de documentos del aplicativo LUCHA.

Control 3

"Socializar la política de seguridad de la SDMujer" no corresponde a una actividad de control, pues no se puede determinar qué tanto del tema socializado quedó interiorizado en los participantes. Por otra parte, es una actividad que se aplicaría con una periodicidad muy larga y por el impacto que podría generar en caso de materialización del riesgo, es indispensable contar con controles de carácter permanente y acordes al volumen de información que es producida por la entidad. Se recomienda analizar si actividad puede ser incluida como acción preventiva para reforzar el tratamiento del riesgo.

Control 4

El control *Documentar el ciclo de vida de los desarrollos de software, in house y/o contratados*, no se encuentra documentado por lo tanto no se identifica un responsable para realizar dicha actividad como punto de control especifico; además, no se evidencia que se haya realizado hasta el momento de la evaluación, la documentación del ciclo de vida de los programas y/o aplicaciones con que cuenta la entidad. Se recomienda revisar dentro de los documentos del proceso de gestión tecnológica, la posibilidad de incluir esta actividad como un punto de control especifico.

Control 5

El control evaluado no presenta documentación relacionada, por lo tanto no se identifica un responsable para realizar dicha actividad como punto de control especifico dentro de los procedimientos y/o los diferentes documentos del proceso de gestión tecnológica.

Analizados los controles identificados para el riesgo, se recomienda tener en cuenta que la formalización, el periodo de aplicación y la identificación de los responsables son atributos muy importantes para una adecuada formulación de controles y en este sentido es necesario revisar todos los documentos relacionadas con el proceso de gestión tecnológica e identificar puntos de control correspondientes. Tal es el caso de los controles que se relacionan en *el Lineamiento para el Alistamiento de Equipos de Cómputo con código GT-LI-01*, dentro del cual en la descripción de actividades se refieren puntualmente a tareas que aportan en la mitigación del riesgo evaluado sobre la pérdida de la información en lo referente a la configuración de equipos de cómputo, en los momentos que se requiera hacer un cambio de hardware o software.

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

Este riesgo cuenta con dos controles a los que se realizó la evaluación de diseño y ejecución (Anexo 1), dando como resultado que el conjunto de controles tiene 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 "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	Fuerte

2	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	**100**: Fuerte	Fuerte	Fuerte	

A continuación, se relaciona el análisis realizado para cada control:

Control No. 1

Cumple con los criterios de diseño en cuanto a su documentación, cuenta con responsables y su frecuencia de aplicación es mensual, adicionalmente no cuenta con hallazgos de auditoría por lo que se considera con una solidez fuerte. Se recomienda articular la periodicidad establecida en el aplicativo LUCHA (mensual) con la periodicidad descrita en el control.

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 No. 2

El control relacionado se encuentra documentado dentro del procedimiento *GT-PR-4 Administración de Backups y Restauración de la Información*, y en cuanto a la periodicidad de su ejecución para el riesgo en evaluación, se evidencia que se aplica mensualmente; es consistente en cuanto su ejecución por parte del responsable que se identifica en el procedimiento y esta coherentemente relacionado con las causas del riesgo. A diferencia de la periodicidad establecida en el riesgo 2 para el desarrollo del control, en esta oportunidad se estableció mensual, por lo que se recomienda unificar los elementos del control en los dos riesgos.

La calificación de los dos controles en su diseño es de 100 puntos, cumpliendo con las características de definición de responsable, oportunidad de aplicación, existencia de evidencia de su ejecución, y documentación del mismo

4.3. ANÁLISIS DE RIESGOS DE CORRUPCIÓN DEL PROCESO GESTIÓN TECNOLOGÍCA

Los riesgos de gestión asociados al proceso "Gestión Tecnología" se presentan en la Tabla 10.

Tabla 10. Riesgos de corrupción del proceso "Gestión Tecnológica " Estructura del riesgo					
Objetivo del proceso: Proveer, gestionar, facilitar, desarrollar e implementar una estrategia de recursos tecnológicos, que permita poner a disposición de toda la SDMujer, una infraestructura tecnológica basada en herramientas informáticas, servicios de redes y comunicaciones que contribuyan a elevar la eficiencia y la efectividad en el cumplimiento de la misión.					
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**

Tabla 10. Riesgos de corrupción del proceso "Gestión Tecnológica " Estructura del riesgo					
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 4.1 del presente informe, en relación con la estructura de los riesgos identificados su puede concluir lo siguiente:

1. Aplicando la metodología del metalenguaje se evidencia que la relación causa – riesgo – consecuencia es coherente y consistente con la estructura de los riesgos formulados.

2. La tipología del riesgo relacionada con los elementos de acción u omisión + uso del poder + desviación de la gestión de lo público + beneficio privado, asociados a corrupción, están coherentes con las consecuencias de la materialización de los riesgos y la temática de que trata el proceso de gestión tecnológica.

3. Para este riesgo también es importante recomendar que se realice un análisis sobre el atributo de *Privacidad de la Información* que se define dentro del habilitador transversal de seguridad de la información la P*olítica de Gobierno Digital (Manual Técnico MIPG)*, esto con el fin de identificar otras causas que podrían dar lugar a controles específicos para el tratamiento del riesgo.

Teniendo en cuenta lo anterior, se procedió a analizar los controles identificados para prevenir la materialización del riesgo o para mitigar sus consecuencias.

4.3.1. Análisis de controles del riesgo "Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad".

Este riesgo cuenta con dos controles a los que se realizó la evaluación de diseño y ejecución (Anexo 1), dando como resultado que el conjunto de controles 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 "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	**100**: Débil	Fuerte	Débil	Débil

2	Establecer control de acceso al centro de computo	**82**: Débil	Moderado	Débil	

A continuación, se relaciona el análisis realizado para cada control:

Control No. 1

Cumple con los criterios de diseño en cuanto a su documentación, cuenta con responsables y su frecuencia de aplicación es mensual, adicionalmente no cuenta con hallazgos de auditoría por lo que se considera con una solidez fuerte. Sin embargo, se recomienda articular la periodicidad establecida en el aplicativo LUCHA (trimestral) con la periodicidad descrita en el control.

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 No. 2

Como se mencionó en el análisis realizado en el numeral 4.2.1., se evidencia que el control cumple con los criterios de diseño en cuanto a su documentación en el aplicativo LUCHA y cuenta con un responsable de su aplicación. No obstante, no se evidencia la segregación de funciones en la aplicación del control. Para la evidencia de su aplicación se encontró que a través del *Manual de Gestión Tecnológica* con código GT-MA-01 y el uso de los formatos *GT-FO-13 – Registro del Ingreso al Centro de Computo - V1 y GT-FO-14 - Solicitud de Acceso al Centro de Computo - V1* se mitiga el riesgo. Sin embargo, y con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis en primera instancia sobre la periodicidad del control (Semestral) y de los puntos de control que se citan dentro del manual, identificando controles específicos y con una periodicidad razonable; esto dado que los riesgos de tipo tecnológico generalmente requieren ser controlados casi que diariamente.

5. CONCLUSIONES

5.1. FORTALEZAS

En desarrollo del seguimiento se identificaron las siguientes fortalezas:

1. Se evidencia relación entre los riesgos identificados y el objetivo del proceso de gestión tecnológica, teniendo en cuenta que la materialización de los riesgos identificados puede afectar negativamente el cumplimiento del objetivo del proceso.

2. El proceso de gestión tecnológica ha venido trabajando en la actualización de su mapa de riesgos y la identificación de sus correspondientes controles en el marco de los seguimientos anteriores realizados por este despacho y teniendo en cuenta los monitoreos realizados durante el seguimiento de ejecución de los controles.

3. El riesgo de corrupción identificado por el proceso cumple con los componentes de acción u omisión + uso del poder + desviación de la gestión de lo público + beneficio privado.

5.2. DEBILIDADES

Las debilidades están compuestas por dos tipos, la oportunidad de mejora y el hallazgo, 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 y tomar medidas y/o decisiones sobre su tratamiento

Nota 1: Las oportunidades de mejora identificadas no requieren un plan de mejoramiento; sin embargo, deben ser atendidas en el marco de la gestión propia del área o proceso responsables, razón por la cual la Oficina de Control Interno revisará las medidas adoptadas para su mitigación en la próxima auditoría. En este sentido, para la formulación de acciones de mejoramiento, se deben tener en cuenta los lineamientos dados desde la Oficina Asesora de Planeación.

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).

Nota 2: Los hallazgos deben ser objeto de formulación de acciones de mejoramiento, tendientes a eliminar de fondo las causas que las originaron, las cuales deben ser formuladas dentro de los ***15 días hábiles*** siguientes a la presentación del Informe de Auditoria. 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.

5.2.1. Oportunidades de Mejora

De acuerdo con la tipología de debilidades a continuación se identifican las oportunidades de mejora evidenciadas en el seguimiento realizado a los riesgos y controles del proceso evaluado:

CUADRO DESCRIPTIVO OPORTUNIDADES DE MEJORA			
No	**DESCRIPCIÓN SITUACIÓN**	**Numeral del Informe**	**Responsable**
1.	Se evidencia la existencia de un procedimiento nombrado *"Gestión de Incidentes de Seguridad de la Información"* GT-PR-09, el cual tiene por objetivo gestionar los incidentes de seguridad de la información que se presenten en la SDMujer con el fin de mitigar riesgos que afecten los elementos de confidencialidad, integridad y disponibilidad de la información. Seria pertinente identificar puntos de control específicos dentro del citado procedimiento para los riesgos formulados, ya que dado su objetivo y alcance articula los atributos que se piden desde los lineamientos genéricos para la Política de Gobierno Digital.	4.2	Oficina Asesora de Planeación
2.	Para la Administración del Riesgo del proceso de gestión tecnológica se recomienda realizar la articulación correspondiente, incluyendo los lineamientos de la Política de Seguridad de la Información que se expidió en	4.2 4.3	Oficina Asesora de Planeación

CUADRO DESCRIPTIVO OPORTUNIDADES DE MEJORA			
No	**DESCRIPCIÓN SITUACIÓN**	**Numeral del Informe**	**Responsable**
	noviembre de la presente vigencia. No se evidencian los controles específicos que enuncia dicha política.		
3.	En cuanto a los controles *1. Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones, 2. Establecer control de acceso al centro de cómputo, 3. Programar el cambio de contraseña de los usuarios cada 45 días y 4. Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer;* que se vienen utilizando dentro del plan de tratamiento para varios de los riesgos del proceso se recomienda revisar los periodos de aplicación que correspondan, dado que se evidencian incoherencias entre los criterios de diseño (procedimientos y aplicativo LUCHA) y ejecución.	4.2 4.3	Oficina Asesora de Planeación
4.	Los tiempos de aplicación de los controles para mitigar algunos de los riesgos son muy largos, por lo que se recomienda identificar controles dentro de los documentos del proceso que se puedan ejecutarse con más frecuencia y sea posible administrar los riesgos mediante puntos de control más específicos que realmente generen un grado de confiabilidad sobre la materialización.	4.2 4.3	Oficina Asesora de Planeación
5.	Es pertinente revisar y/o actualizar los documentos asociados a los controles, incluyéndolos como puntos de control en los procedimientos, manuales, guías, instructivos entre otros, según corresponda.	4.2 4.3	Oficina Asesora de Planeación
6.	Nuevamente y con base en evaluaciones anteriores, se recomienda tener en cuenta los controles operacionales que establece la norma técnica 27001 para el Sistema de Seguridad de la Información, ya que estos se ajustan a los documentos con que cuenta el proceso de gestión tecnológica y están acorde con lo establecidos por las políticas gubernamentales.	4.2 4.3	Oficina Asesora de Planeación

5.2.2. *Hallazgos*

No se evidenciaron hallazgos de auditoria asociados al seguimiento realizado.

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

NORHA CARRASCO RINCON
JEFA DE CONTROL INTERNO

ANEXO 1. MATRIZ DE RIESGOS GESTIÓN TECNOLÓGICA

RIESGOS			CONTROLES																		
							EVALUACIÓN DEL DISEÑO DE CONTROLES									EVALUACION DE LA EJECUCION DEL CONTROL			SOLIDEZ DEL CONTROL		
ID LUCHA	Nombre	Procesos	ID	Control	Periodicidad de ejecución	Tipo de control	Responsable	¿Responsable con autoridad y adecuada segregación de funciones?	Periodicidad	Propósito	¿Fuente de información es confiable?	¿Evidencia o rastro de la ejecución?	¿Documentado en LUCHA?	EVALUACIÓN DISEÑO		Ejecucion del control	Materialización y/o Hallazgos	EVALUACIÓN EJECUCIÓN	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	OBSERVACIONES FINALES
														Puntaje	Clasificación						
		- GESTION TECNOLOGICA	248	Realizar escaneos técnicos de vulnerabilidades a la infraestructura tecnológica: Monitorear las amenazas que puedan vulnerar los equipos de cómputo, es? como la información de la entidad	Mensual	Preventivo	No Asignado	Inadecuado	Oportuna	Detectar	No Confiable	Incompleta	NO	35	DEBIL	El control no se ejecuta por parte del responsable	NO	DEBIL	DEBIL		El control evaluado no presenta documentación relacionada, por lo tanto no se identifica un responsable para realizar dicha actividad como punto de control específico dentro de los procedimientos y/o los diferentes documentos del proceso de gestión tecnológica.
86	Eliminar y modificar información en las aplicaciones y bases de datos de la SDMujer.	- GESTION TECNOLOGICA	175	Programar el cambio de contrase?a de los usuarios cada 45 d?as	Mensual	Correctivo	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Completa	SI	100	FUERTE	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	FUERTE	FUERTE	Es pertinente revisar y/o actualizar los documentos asociados a los controles, dado que se evidencia que existen procedimientos que relacionan actividades que podrían llegar a formularse como puntos de control según corresponda. Se recomienda revisar incluyendo los lineamientos de la Política de Seguridad de la información que se expidió en noviembre de la presente vigencia.
		- GESTION TECNOLOGICA	176	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	Mensual	Preventivo	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Completa	SI	100	FUERTE	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	FUERTE	FUERTE	Es pertinente revisar y/o actualizar los documentos asociados a los controles, dado que se evidencia que existen procedimientos que relacionan actividades que podrían llegar a formularse como puntos de control según corresponda. Se recomienda revisar incluyendo los lineamientos de la Política de Seguridad de la información que se expidió en noviembre de la presente vigencia.
115	Acceso indebido a los sistemas de información y/o servidores de dominio de la Entidad	- GESTION TECNOLOGICA	274	Programar el cambio de contrase?a de los usuarios cada 45 d?as	Trimestral	Preventivo	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Completa	SI	100	FUERTE	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	FUERTE	MODERADO	Cumple con los criterios de diseño en cuanto a su documentación y cuenta con responsables para su ejecución. Sin embargo, se recomienda ajustar la periodicidad en el aplicativo LUCHA (Trimestral), pues no es coherente con la periodicidad de aplicación del control. 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.
		- GESTION TECNOLOGICA	275	Establecer control de acceso al centro de computo	Trimestral	Preventivo	Asignado	Inadecuado	Inoportuna	Prevenir	Confiable	Completa	SI	67	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL		El riesgo tiene dos controles que se encuentran documentados y tienen un responsable, pero en cuanto a la periodicidad de su aplicación, tiene un tiempo muy largo de ejecución; lo cual podría generar la materialización del riesgo. Por esto es recomendable analizar el periodo de tiempo para la aplicación consistente con el impacto del riesgo. Po otro lado, es pertinente revisar y/o actualizar los documentos asociados a los controles, dado que se evidencia que existen procedimientos que relacionan actividades que podrían llegar a formularse como puntos de control según corresponda. Se recomienda revisar incluyendo los lineamientos de la Política de Seguridad de la Información que se expidió en noviembre de la presente vigencia.

ANEXO 1. MATRIZ DE RIESGOS GESTIÓN TECNOLÓGICA

RIESGOS			CONTROLES																		
							EVALUACIÓN DEL DISEÑO DE CONTROLES									EVALUACION DE LA EJECUCION DEL CONTROL			SOLIDEZ DEL CONTROL		
ID LUCHA	Nombre	Procesos	ID	Control	Periodicidad de ejecución	Tipo de control	Responsable	¿Responsable con autoridad y adecuada segregación de funciones?	Periodicidad	Propósito	¿Fuente de información es confiable?	¿Evidencia o rastro de la ejecución?	¿Documentado en LUCHA?	EVALUACIÓN DISEÑO		Ejecucion del control	Materialización y/o Hallazgos	EVALUACIÓN EJECUCIÓN	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	OBSERVACIONES FINALES
														Puntaje	Clasificación						
82	Caidas de red (Comunicaciones, Internet, Sistemas)	- GESTION TECNOLOGICA	163	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Anual	Preventivo	Asignado	Adecuado	Oportuno	Prevenir	Confiable	Completa	SI	100	FUERTE	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	MODERADO	DEBIL	Está documentado dentro del instructivo nombrado Plan de Mantenimiento Preventivo a Equipos Informáticos con código GT-PL-01 especificando los responsables de llevarlo a cabo y para algunas actividades se identifica su periodicidad . El control identificados para el riesgos tienen una periodicidad muy larga para su aplicación (anual), lo cual implica que puede existir una brecha para la materialización del riesgo, dado que el impacto de ocurrencia puede llegar a ser ALTO para la gestión propia de la entidad y adicionalmente puede desencadenar en que se materialicen otros riesgos como el de perdida de la información. Por esta razón se recomienda analizar la pertinencia de los controles formulados por parte del proceso de gestión tecnológica.
		- GESTION TECNOLOGICA	165	Establecer control de acceso al centro de computo	Semestral	Preventivo	Asignado	Inadecuado	Inoportuna	Prevenir	Confiable	Completa	SI	67	DEBIL	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	DEBIL		El control "Establecer control de acceso al centro de cómputo", cumple con los criterios de diseño en cuanto a su documentación en el aplicativo LUCHA y cuenta con un responsable de su aplicación. No obstante, no se evidencia la segregación de funciones en la aplicación del control. Para la evidencia de su aplicación se encontró que a través del Manual de Gestión Tecnológica con código GT-MA-01 y el uso de los formatos GT-FO-13 – Registro del Ingreso al Centro de Computo - V1 y GT-FO-14 - Solicitud de Acceso al Centro de Computo - V1 se mitiga el riesgo. Sin embargo, y con el ánimo de mejorar el blindaje sobre la ocurrencia o materialización del riesgo, se recomienda realizar un análisis en primera instancia sobre la periodicidad del control (Semestral) y de los puntos de control que se citan dentro del manual, identificando controles específicos y con una periodicidad razonable; esto dado que los riesgos de tipo tecnológico generalmente requieren ser controlados casi que diariamente.
83	Perdida de informaci?n confidencial	- GESTION TECNOLOGICA	166	Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.	Anual	Preventivo	Asignado	Adecuado	Oportuna	Prevenir	Confiable	Completa	SI	100	FUERTE	El control se ejecuta algunas veces por parte del responsable.	NO	MODERADO	MODERADO	DEBIL	Está documentado dentro del instructivo nombrado Plan de Mantenimiento Preventivo a Equipos Informáticos con código GT-PL-01 especificando los responsables de llevarlo a cabo y para algunas actividades se identifica su periodicidad . El control identificados para el riesgos tienen una periodicidad muy larga para su aplicación (anual), lo cual implica que puede existir una brecha para la materialización del riesgo, dado que el impacto de ocurrencia puede llegar a ser ALTO para la gestión propia de la entidad y adicionalmente puede desencadenar en que se materialicen otros riesgos como el de perdida de la información. Por esta razón se recomienda analizar la pertinencia de los controles formulados por parte del proceso de gestión tecnológica.
		- GESTION TECNOLOGICA	167	Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer	Anual	Preventivo	Asignado	Inadecuado	Oportuna	Prevenir	Confiable	Completa	SI	85	DEBIL	El control se ejecuta de manera consistente por parte del responsable	NO	FUERTE	DEBIL		El control relacionado se encuentra documentado dentro del procedimiento GT-PR-4 Administración de Backups y Restauración de la Información, que para la aplicación de sus actividades se observa una inadecuada segregación de funciones dado que no se evidencia un responsable con autoridad para avalar el cumplimento de los lineamientos para realizar los respectivos backups. Por otra parte, y en cuanto a la periodicidad de su ejecución para el riesgo en evaluación, se evidencia que al tener periodos de aplicación del control tan largos (Anual), la perdida de información se puede materializar en cualquier momento En cuanto a la normatividad que enuncia el procedimiento GT-PR-4 Administración de Backups y Restauración de la Información, se recomienda actualizar los documentos que allí se relacionan, ya que se identifica un Protocolo de Administración de Backup código GT-IN-1 que ya no se encuentra dentro del listado de documentos del proceso de gestión tecnológica ni aparece en el módulo de documentos del aplicativo LUCHA.
		- GESTION TECNOLOGICA	168	Socializar la política de seguridad de la SDMujer	Anual	Preventivo				No es un control				0	DEBIL				DEBIL		No es una actividad de control, pues no se puede determinar con certeza qué tanto del tema socializado quedó interiorizado en los participantes.
		- GESTION TECNOLOGICA	247	Documentar el ciclo de vida de los desarrollos de software, in house y/o contratados.	Mensual	Preventivo	No Asignado	Inadecuado	Oportuna	Prevenir	No Confiable	Incompleta	NO	40	DEBIL	El control no se ejecuta por parte del responsable	NO	DEBIL	DEBIL		El control Documentar el ciclo de vida de los desarrollos de software, in house y/o contratados, no se encuentra documentado por lo tanto no se identifica un responsable para realizar dicha actividad como punto de control específico; además, no se evidencia que se haya realizado hasta el momento de la evaluación, la documentación del ciclo de vida de los programas y/o aplicaciones con que cuenta la entidad. Se recomienda revisar dentro de los documentos del proceso de gestión tecnológica, la posibilidad de incluir esta actividad como un punto de control específico.