1. NOMBRE DE LA POLÍTICA: Política de Administración de Riesgos.

2. OBJETIVO

Establecer los lineamientos para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de gestión, de corrupción y de seguridad digital, con el fin de prevenir de forma anticipada su ocurrencia y minimizar el impacto que pueda afectar el logro de los objetivos Institucionales.

3. ALCANCE

La responsabilidad de la administración de los riesgos aplica a todos los procesos y proyectos de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC. Incluye riesgos de gestión, corrupción y seguridad digital.

4. TÉRMINOS Y DEFINICIONES[1]

Aceptar el Riesgo: decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Acción Correctiva: acción tomada para eliminar y/o mitigar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

Acción Preventiva: acción tomada para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

Activo: se considera cualquier elemento que tiene valor para la organización. Para la Gestión de Riesgos de Seguridad digital en la USPEC hace referencia a toda aquella información física y digital gestionada a través de su software, hardware, servicios y recurso humano de la Entidad.

Amenaza: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Control: medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Control Correctivo: aquel que permite el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Control Preventivo: aquel que actúa para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

Corrupción: uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera un usuario autorizado.

[1] Función Pública 2018, Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4.

Efectos: constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y vulneración de los derechos de las personas privadas de la libertad, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Evaluación del Riesgo: proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

Impacto: consecuencias o efectos que puede generar la materialización del riesgo en la entidad.

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: propiedad de la información relativa a su exactitud y completitud.

Mapa de Riesgos: documento con la información resultante de la administración del riesgo.

Probabilidad: posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo de gestión: posibilidad de que suceda un algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo Inherente el que resulta de la ausencia de acciones para modificar su probabilidad o impacto.

Riesgo Residual: nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

Tolerancia al riesgo: niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. DISPOSICIONES GENERALES

Este documento describe la metodología y establece los lineamientos para la administración de los riesgos de gestión, corrupción, y seguridad digital para la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, y

adopta la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública - DAFP.

- Los lineamientos de la política de administración de riesgos de la USPEC son establecidos por la Alta Dirección en cabeza de la Dirección General, y con la participación del Comité Institucional de Coordinación de Control Interno.

- La identificación de riesgos y su actualización deben tener en cuenta como insumo la misión, visión, objetivos estratégicos, metas, planes, proyectos y las prioridades de la Entidad, incluyendo las del plan de desarrollo vigente. Adicionalmente, se debe tener en cuenta el contexto organizacional, caracterizaciones de los procesos, informes de entes de control y de la Oficina de Control Interno.

- La identificación, análisis, valoración y administración de los riesgos (gestión, corrupción y seguridad digital) debe realizarse a todos los procesos.

- Para el levantamiento, actualización y seguimiento de los riesgos de gestión, corrupción y de seguridad digital se debe utilizar la G1-S3-FO-08 “Herramienta de Administración de Riesgos”.

- Los riesgos de seguridad digital, se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información.

- Los riesgos (gestión, corrupción y seguridad digital) deben ser elaborados y/o revisados anualmente por los responsables de procesos y su equipo, antes del inicio de cada vigencia.

- La identificación o actualización de activos de información se debe realizar teniendo en cuenta los lineamientos establecidos en el A3-MA-02 Manual de Clasificación de Activos.

- Los riesgos de seguridad digital se analizarán para aquellos activos valorados como "Críticos" y "Altos".

6. RESPONSABILIDADES

6.1 RESPONSABILIDAD DE LA LÍNEA ESTRATÉGICA (Alta Dirección y Comité Institucional de Control Interno)

- Definir y aprobar los lineamientos para la gestión del riesgo y el control, y supervisar su cumplimiento en acompañamiento del Comité Institucional de Coordinación de Control Interno.

- Revisar los cambios que se generen en el contexto de la Entidad y que puedan desplegar nuevos riesgos o modificación de los ya identificados.

- A través del Comité Institucional de Control Interno realizar seguimiento a la gestión del riesgo y a los resultados de las evaluaciones que realiza la Oficina de Control Interno y de auditorías internas.

- Tener en cuenta los incidentes de seguridad digital que hayan afectado a la Entidad, para la toma de decisiones en el proceso de revisión de los riesgos.

6.2 RESPONSABILIDAD DE LA PRIMERA LÍNEA DE DEFENSA (líderes de proceso y de proyectos)

- Identificar, valorar y actualizar cuando sea necesario, los riesgos que puedan afectar los planes, proyectos y procesos a su cargo, enfatizando en la prevención del daño antijurídico.

- Definir, implementar y hacer seguimiento a los controles para mitigar los riesgos identificados, y que contribuyan al cumplimiento de las metas y objetivos de la Entidad. Detectar las deficiencias de los controles y establecer las acciones de mejora correspondientes.

- Informar a la Oficina Asesora de Planeación y Desarrollo, y a la Dirección General, cuando se presente la materialización de riesgos en los planes, proyectos o procesos a su cargo.

- Reportar los avances y evidencias de la gestión de los riesgos a cargo.

- Realizar seguimiento cada tres meses a los riesgos en la G1-S3-FO-08 "Herramienta de Administración de Riesgos", y reportarlo a la Oficina Asesora de Planeación y Desarrollo y a la Oficina de Control Interno con las evidencias correspondientes de la gestión.

- Revisar los riesgos del proceso durante el último trimestre de cada año, para su actualización, aprobación y publicación en el portal web institucional máximo el 31 de enero de la siguiente vigencia.

6.3 RESPONSABILIDAD DE LA SEGUNDA LÍNEA DE DEFENSA (Oficina Asesora de Planeación y Desarrollo, responsables de sistemas de gestión)

- Liderar el proceso de administración de los riesgos y consolidar el mapa de riesgos institucional (riesgos de mayor criticidad y/o relevantes frente al logro de los objetivos).

- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.

- Dar a conocer a funcionarios y contratistas el mapa de riesgos antes de su publicación. De igual manera se debe dar a conocer a la ciudadanía y partes interesadas (población objeto identificada). Se deben conservar las evidencias de la socialización, así como consolidar y publicar los aportes recibidos.

- Publicar el mapa de riesgos máximo el 31 de enero de cada vigencia, en la sección de transparencia y acceso a la información.

- Definir condiciones de reserva y clasificación de elementos constitutivos del mapa de riesgos.

- Acompañar a los líderes de procesos en las modificaciones a los riesgos y dejar trazabilidad de las modificaciones realizadas.

- Monitorear la implementación de los controles definidos por la primera línea de defensa, teniendo en cuenta la información suministrada por los líderes de procesos.

- Evaluar que los riesgos identificados por la primera línea de defensa cumplan con los lineamientos definidos.

- Realizar seguimiento trimestral y consolidar los avances y actualizaciones al mapa de riesgos, y publicar en página web.

- Realizar divulgación y socialización de los mapas de riesgos por proceso y el Mapa de Riesgos Institucional aprobados, al interior de la Entidad.

- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Nota: Para los riesgos de seguridad digital, el acompañamiento, seguimiento, monitoreo y consolidación lo realiza la Oficina de Tecnología, y remite las modificaciones y seguimientos a la Oficina Asesora de Planeación y Desarrollo.

6.4 RESPONSABILIDAD DE LA TERCERA LÍNEA DE DEFENSA (Oficina de Control Interno)

- Asesorar en coordinación con la Oficina Asesora de Planeación y Desarrollo y la Oficina de Tecnología, a la primera línea de defensa en la identificación, análisis y valoración del riesgo, y en el diseño de los controles.

- Verificar la publicación del mapa de riesgos en el portal web institucional.

- Realizar seguimiento a la gestión de riesgos (analizar causas, riesgos, eficacia y efectividad de los controles), en los procesos que realice de auditorías internas.

- Recomendar mejoras a la política de administración del riesgo.

- Realizar monitoreo y evaluación a la gestión de riesgos por lo menos dos veces al año, una por semestre.

- Realizar seguimiento a los riesgos de corrupción cada cuatro meses y publicarlo en la página web de la Entidad para consulta, de la siguiente manera:

  Primer corte 30 de abril: se publica dentro de los diez (10) primeros días hábiles del mes de mayo.
  Segundo corte 31 de agosto: se publica dentro de los diez (10) primeros días hábiles del mes de septiembre.
  Tercer corte al 31 de diciembre: se publica dentro de los diez (10) primeros días hábiles del mes de enero.

7. METODOLOGÍA

La metodología para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de la Entidad, está basada en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del DAFP, su "Anexo 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" de MinTIC, o el documento que lo sustituya; para mayor detalle puede consultar el documento en la página web del DAFP. Los pasos y lineamientos específicos para la USPEC, son los siguientes:

7.1 IDENTIFICACIÓN DE RIESGOS

Previo a la identificación de los riesgos, la Oficina Asesora de Planeación y Desarrollo debe revisar los objetivos estratégicos y los objetivos de los procesos; debe validar que los objetivos en su descripción o redacción den respuesta a las siguientes preguntas: ¿qué se quiere lograr?, ¿para qué quiere lograrlo?, ¿cómo quiere lograrlo?, ¿cuándo piensa lograrlo? y ¿cuánto avance debo cumplir en cada vigencia?

La identificación del riesgo se debe registrar en la hoja "Identificación riesgo" de la G1-S3-FO-08 "Herramienta de Administración de Riesgos".

7.1.1 Establecimiento del contexto

Los líderes de procesos deben establecer el contexto interno y externo de la Entidad, el contexto de los procesos y los activos de seguridad digital. Los factores para cada categoría son:

FACTORES	
CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.

	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

7.1.2 Identificación del riesgo

Luego de establecer el contexto (incluyendo causas y consecuencias) se deben identificar los riesgos, que son aquellos eventos o situaciones que pueden llegar a entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos. Para ello, es necesario responder las siguientes preguntas para la identificación: ¿qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder? y ¿Qué consecuencias tendría su materialización?, y con las respuestas construir la descripción del riesgo.

Luego se deben identificar las causas del riesgo que pueden afectar el logro de los objetivos y las consecuencias o efectos resultantes de la materialización de un riesgo que afecte los objetivos del proceso, la entidad o partes interesadas. También se deben identificar las amenazas y vulnerabilidades de los activos de información que generen riesgos de seguridad digital. Se debe tener conocimiento general del proceso y tener acceso o conocimiento de datos y hechos históricos de la Entidad para realizar una completa identificación.

Para la identificación de los activos de información es necesario considerar los lineamientos establecidos en el A3-MA-02 “Manual de Clasificación de Activos”.

En la descripción de riesgos de corrupción, es preciso atender al cumplimiento de los siguientes componentes: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado. La descripción del riesgo debe ser clara y precisa, y para clasificarse como riesgo de corrupción debe cumplir con las cuatro condiciones.

Para cada riesgo de seguridad digital se deben vincular los activos relacionados y se deben evaluar amenazas y vulnerabilidades que pueden causar la materialización del riesgo (ver como referencia el listado contenido en la G1-S3-FO-08 Herramienta de Administración de Riesgos, hoja “Listas y conceptos”). Se pueden identificar tres riesgos de seguridad digital:

- Pérdida de confidencialidad.
- Pérdida de integridad.
- Pérdida de disponibilidad.

7.2 VALORACIÓN DE RIESGOS (análisis y evaluación)

En esta fase se define la probabilidad de ocurrencia del riesgo (eventos positivos y/o negativos) y su consecuencia o impacto para estimar la zona de riesgo inicial (riesgo inherente antes del diseño de controles), y luego comparar los resultados frente a los controles, diseñados y evaluados, para determinar la zona de riesgo final (riesgo residual) y determinar de acuerdo a las capacidades de la Entidad, su aceptación y tratamiento.

7.2.1 Análisis de riesgos

El objetivo es analizar la posibilidad de ocurrencia del riesgo, y expresarla en términos de frecuencia (hechos que se han materializado) o factibilidad (hechos que no se ha presentado pero es posible que suceda). Los criterios para calificar la probabilidad son:

CRITERIOS PARA CALIFICAR LA PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DECRIPCIÓN**	**FRECUENCIA**
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Los criterios para calificar el impacto para los riesgos de gestión, corrupción y seguridad digital, se encuentran vinculados en la G1-S3-FO-08 Herramienta de Administración de Riesgos (hojas “Impacto RG”, “Impacto RC” e “Impacto RSD” respectivamente).

Con el resultado de la calificación del riesgo, se ubica el impacto y probabilidad en el mapa de calor, para determinar el nivel de riesgo, y como resultado se obtiene el ***riesgo inherente***:

Matriz de Calificación, Evaluación y Respuesta a Riesgos					
Impacto	**Insignificante**	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Probabilidad	1	2	3	4	5
Raro 1	**Bajo**	**Bajo**	**Medio**	**Alto**	**Extremo**
Improbable 2	**Bajo**	**Bajo**	**Medio**	**Alto**	**Extremo**
Posible 3	**Bajo**	**Medio**	**Alto**	**Extremo**	**Extremo**
Probable 4	**Medio**	**Alto**	**Alto**	**Extremo**	**Extremo**
Casi Seguro 5	**Alto**	**Alto**	**Extremo**	**Extremo**	**Extremo**

Extremo	Reducir el riesgo, Evitar, Compartir o Transferir.
Alto	Reducir el riesgo, Evitar, Compartir o Transferir.
Moderado	Asumir el Riesgo, Reducir el Riesgo.
Bajo	Asumir el Riesgo.

Nota: Para los riesgos de corrupción solo aplican las columnas de Impacto Moderado, Mayor y Catastrófico.

7.2.2 Evaluación de riesgos

Para esto es necesario diseñar los controles para mitigar de manera adecuada el riesgo. La descripción del control debe contener las variables incluidas en la G1-S3-FO-08 Herramienta de Administración de Riesgos (hoja "Valoración riesgos"): responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, y evidencia. Para cada causa debe existir un control.

Luego del diseño de los controles, se debe valorar si está bien diseñado para mitigar el riesgo y si se ejecuta como fue diseñado y es consistente. Los rangos de calificación del diseño son los siguientes:

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Si la calificación del control o el promedio en el diseño de los controles están por debajo de 96% se debe generar un plan de acción, donde se establezcan controles bien diseñados (criterios definidos en la G1-S3-FO-08 Herramienta de Administración de Riesgos). Adicionalmente, se debe evaluar la ejecución de cada control, el cual puede ser Fuerte, Moderado o Débil, y luego evaluar la solidez del control, de acuerdo a los siguientes valores: (a) Fuerte: 100; (b) Moderado: 50; y (c) Débil: 0.

Posterior a la evaluación de los controles individuales, se debe evaluar el conjunto de controles asociados a cada riesgo. La solidez del conjunto de los controles se califica de acuerdo a los siguientes valores:

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Nota: Ningún riesgo con medida de tratamiento se evita o elimina.

Finalmente, de acuerdo con los resultados de la evaluación realizada a la solidez del conjunto de los controles, se debe determinar el desplazamiento del riesgo en el mapa de calor, si disminuyen la probabilidad o el impacto. Para el caso de riesgos de corrupción únicamente disminuye la probabilidad, no debe haber desplazamiento en el impacto.

7.2.3 Tratamiento del riesgo

La primera línea de defensa es la responsable de definir las acciones de tratamiento para mitigar los riesgos identificados (Plan de Tratamiento de Riesgos). Para los riesgos de corrupción las opciones de tratamiento después de la valoración de controles solo deben ser: evitar, compartir o reducir el riesgo.

Todos los riesgos con evaluación después de controles que se encuentren en zona “Alta” y “Extrema”, deben definir acciones para el tratamiento de los riesgos. Las opciones de tratamiento y los lineamientos para cada uno son:

- **Aceptar el riesgo:** no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Esto debe aplicar para riesgos inherentes calificados como “bajo” ya que no es necesario poner controles o no es posible aplicar controles. Para esta opción de tratamiento se debe realizar seguimiento continuo al riesgo *(Ningún riesgo de corrupción debe ser aceptado)*.

- **Reducir el riesgo:** se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

- **Evitar el riesgo:** se abandonan las actividades que dan lugar al riesgo, es decir, no dar inicio o no continuar con la actividad que lo provoca.

- **Compartir el riesgo:** se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no transferir su responsabilidad. Las opciones más utilizadas para esta situación es que la Entidad adquiera seguros y/o realice la tercerización que aumenta la probabilidad del riesgo, y en caso de decidir esta opción de tratamiento, debe estar formalizada a través de un acuerdo contractual.

Para tratar o mitigar los riesgos de seguridad digital, se deben tomar como referencia los controles establecidos en el Anexo A de la Norma ISO 27001:2013. (El listado de controles se encuentra como información adicional en la G1-S3-FO-08 Herramienta de Administración de Riesgos, hoja "Anexo A 27001"). Una vez se implementen estos controles, debe actualizarse el documento que contiene la declaración de aplicabilidad de la Entidad, con el fin de incluir en cada control los soportes de su implementación. Esta tarea está a cargo del responsable de riesgos en seguridad digital de la Entidad.
Es preciso definir actividades de control para prevenir que el riesgo se materialice, y si llega a pasar, debe ser detectado de manera oportuna. Los tipos de controles son:

- Preventivos: diseñados para evitar la ocurrencia de riesgos que afecten el cumplimiento de los objetivos.

- Detectivos: diseñados para detectar la situación no deseada, se corrija y se tomen las acciones correspondientes.

Los mapas de riesgos, que incluyen Planes de Tratamiento de Riesgos y la aceptación de los riesgos residuales, deben ser aprobados por los líderes de proceso a través de acta o correo electrónico.

Después de definidos los mapas de riesgos de todos los procesos, la Oficina Asesora de Planeación y Desarrollo debe consolidar y generar el mapa de riesgos Institucional, el cual debe contener los riesgos de gestión, corrupción y seguridad digital. El mapa debe ser aprobado en Comité Institucional de Control Interno, para su posterior socialización y publicación.

7.3 MONITOREO Y REVISIÓN

- El Mapa de riesgos de proceso, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso.

- El responsable del proceso deben verificar que los controles establecidos en el plan de tratamiento de riesgos operen de manera adecuada para mitigar los riesgos.

- El seguimiento de los riesgos identificados (incluyendo el plan de tratamiento) se debe realizar de manera trimestral por cada uno de los líderes de los procesos, quienes reportarán a la Oficina Asesora de Planeación y Desarrollo (Riesgos de Gestión y Corrupción) y la Oficina de Tecnología (Riesgos de Seguridad Digital) los avances en las acciones y las evidencias correspondientes en la G1-S3-FO-08 "Herramienta de Administración de Riesgos".

- En caso de materialización de un riesgo, el responsable del proceso debe generar una acción correctiva de acuerdo con el procedimiento G1-S3-PR-02 "Acciones Correctivas, Preventivas y de Mejora", y debe revisar nuevamente la identificación del riesgo, el diseño y valoración de controles, y el plan de tratamiento para mitigar el riesgo.

- Anualmente se debe realizar la valoración de los riesgos de gestión, corrupción y seguridad digital con el fin de verificar que los planes de tratamiento fueron efectivos y los niveles de riesgo disminuyeron.

- El responsable realizar el seguimiento a los riesgos de seguridad digital debe reportar semestralmente a la Dirección General el estado de los mismos.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	28/04/2015	Todos	Se crea el documento
02	10/03/2016	Todos	Se actualizan todos los numerales del documento y se introducen los lineamientos Institucionales para la gestión del riesgo de corrupción
03	17/10/2019	Todos	Se actualizan todos los numerales acorde a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado
Nombre: Paula Viviana Olaya González	Nombre: Katherin Díaz Albarracín	Nombre: Katherin Díaz Albarracín
Cargo: Contratista	Cargo: Jefe Oficina de Planeación y Desarrollo	Cargo: Jefe Oficina de Planeación y Desarrollo
Dependencia: Oficina Asesora de Planeación y Desarrollo	Dependencia: Oficina Asesora de Planeación y Desarrollo	Dependencia: Oficina Asesora de Planeación y Desarrollo
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Oscar Javier Suárez Ramos	Nombre: Oscar Javier Suárez Ramos
Cargo: Profesional Especializado	Cargo: Jefe Oficina Tecnología	Cargo: Jefe Oficina Tecnología
Dependencia: Oficina Tecnología	Dependencia: Oficina Tecnología	Dependencia: Oficina Tecnología