Política para la Administración del Riesgo y el Diseño De Controles - Riesgos de Gestión, Corrupción y Seguridad Digital

ELABORO: Carlos Samuel Rosado Sarabia **Oficina de Calidad**	REVISO: Stella Medina Solano. **Representante de la Alta Dirección**	JUAN JOSE MUÑOZ ROBAYO **Gerente** APROBO: **RESOLUCIÓN No. 340 de 2021/06/25**
FECHA: 2021/06/23	FECHA: 2021/06/23	
Vo.Bo: Martha E. Amaya G. **Oficina de Calidad**	FECHA: 2021/06/24	

CONTENIDO

LINEAMIENTOS DE LA POLÍTICA DE RIESGOS.

La metodología que se utilizará para el establecimiento de la política de administración de riesgos será la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (versión 5), del Departamento Administrativo de la Función Pública.

Política para la gestión del riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo[1].

Gestión del riesgo: La gestión o Administración del riesgo Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo[2].

Riesgo. Efecto de la incertidumbre sobre los objetivos[3]. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos.

La establece la Alta Dirección de la entidad. Con el liderazgo del Representante Legal y la participación del Comité Institucional de Coordinación de Control Interno.

Se debe tener en cuenta los Objetivos estratégicos de la entidad, Niveles de Responsabilidad frente al manejo de riesgos, Mecanismos de comunicación utilizados para dar a conocer la política de riesgo en todos los niveles de la entidad.

Objetivo: Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.

Alcance: La Administración de Riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información (Ver Caja de Herramientas).

Niveles de aceptación al riesgo: Decisión informada de tomar un riesgo particular[4]. Para riesgos de corrupción es inaceptable.

Niveles para Calificar el Impacto: Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).

[1] NTC ISO31000 Numeral 2.4.
[2] NTC ISO31000 Numeral 2.1
[3] NTC ISO31000 Numeral 2.1
[4] NTC GTC137, Numeral 3.7.1.6

Tratamiento de riesgos: Proceso para modificar el riesgo[5].

Periodicidad para el seguimiento: De acuerdo con el nivel de riesgo residual.

MIPG establece que esta es una tarea propia del equipo directivo y se debe hacer desde el ejercicio de Direccionamiento Estratégico y de Planeación. En este punto, se deben emitir los lineamientos precisos para el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

Adicional a los riesgos operativos, es importante identificar los riesgos de corrupción (que se tratarán en el Plan Anticorrupción que defina la entidad), los riesgos de contratación, los riesgos para la defensa jurídica, los riesgos de seguridad digital entre otros.

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo.

Los Riesgos aceptados están sujetos a monitoreo.

La mitigación de los riesgos se hará mediante un plan de acción.

[5] NTC GTC137, Numeral 3.8.1

1. OBJETIVO.

Establecer una metodología que permita orientar la toma de decisiones oportunas y minimizar las consecuencias negativas en la Empresa Social del Estado del Departamento del meta E.S.E "Solución Salud", en la gestión de los procesos, con el propósito de salvaguardar la gestión institucional y asegurar el cumplimiento de los compromisos con los ciudadanos, servidores y entes de control mediante la correcta administración de sus riesgos (de gestión, de corrupción y de seguridad digital), los cuales pueden afectar el cumplimiento de los objetivos institucionales.

2. ALCANCE Y RESPONSABLES.

2.1 ALCANCE.

Los lineamientos presentados en este documento aplican para todas las dependencias, procesos y actividades ejecutada por los funcionarios y contratistas de la Empresa Social del Estado del Departamento del meta E.S.E "Solución Salud".

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos: de proceso, de corrupción y de seguridad digital, los cuales inician con las actividades de identificación de los riesgos incluyendo el análisis, valoración, monitoreo, evaluación y seguimiento de estos.

2.2 RESPONSABLES.

La Alta Dirección y el Comité de Coordinación del Sistema de control Interno: Son los responsables de definir de la Política de Administración de Riesgos para la entidad, la cual es aprobada por el representante legal.

Líderes de proceso: Son los responsables de identificar, analizar y valorar los riesgos de gestión, de corrupción y de seguridad digital con el apoyo de sus grupos de trabajo y actualizarlos cuando se requiera, con el acompañamiento, orientación y entrenamiento de la oficina de Planeación.

Oficina Asesora de Planeación: Asesora a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.

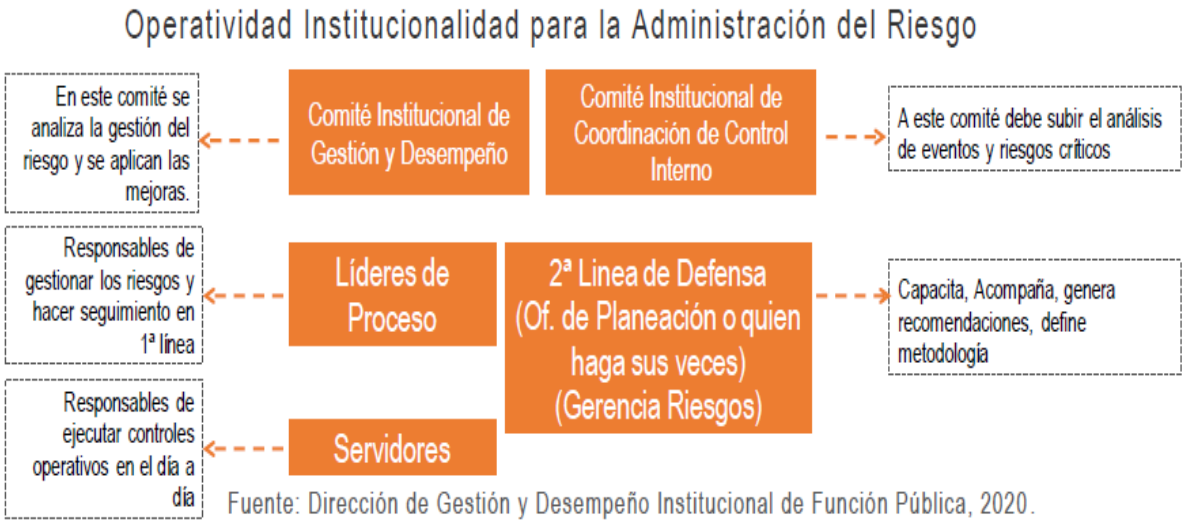
Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y tramita su aprobación.

La Oficina de Planeación realiza el seguimiento semestral a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad al Comité Institucional de Coordinación de Control Interno.

Oficina de Control Interno: Proporciona aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos y proporciona aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa y asesora de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. Adicionalmente, recomienda mejoras a la política de administración del riesgo.

Oficina Asesora jurídica: Es la responsable en la identificación, análisis, valoración y seguimiento de los riesgos en todos los procesos contractuales que se realicen de acuerdo con las disposiciones establecidas en el estatuto y manual de contratación de la ESE (Ver Numeral 6: Registro de Calidad).

Oficina de Sistemas: Es la responsable en la identificación, análisis, valoración y seguimiento de los riesgos seguridad digital de acuerdo con el Modelo de Gestión de Riesgos de Seguridad Digital -MGRSD- del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC.



3. GENERALIDADES.

3.1 RIESGOS POR PROCESOS.

3.1.1. PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS:

"*Establecer los parámetros necesarios para una adecuada **administración** de **riesgos** a través de los siguientes elementos: contexto estratégico, identificación de **Riesgos**, análisis de **riesgos**, valoración de **riesgos**. El monitoreo y seguimiento de los riesgos se hará en aquellos cuya **Zona de riesgo residual** sea moderada o superior*".

1. **Establecimiento del contexto:** Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo[6]. Se debe establecer el contexto interno, externo de la entidad, el contexto del proceso y sus activos de seguridad digital. Es posible hacer uso de herramientas y técnicas (consultar Anexo 2. Técnicas para Establecimiento del Contexto y Valoración del Riesgo).

1.1 Contexto interno: Se refiere a las características, condiciones y aspectos esenciales del ambiente de trabajo en el cual la organización busca alcanzar sus objetivos. Se pueden considerar entre otros factores como:

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.

1.2 Contexto externo: Hace referencia a las características o aspectos esenciales de los elementos que pueden formar parte del entorno en el cual opera la entidad. Se pueden considerar entre otros factores como:

ECONÓMICOS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación.
SOCIALES: Demografía, responsabilidad social, orden público.
TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

[6] NTC ISO31000, Numeral 2.9

COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

1.3 Contexto del proceso: Son los parámetros básicos dentro de los cuales se deben gestionar los **riesgos** y establece el alcance y criterios para el resto del **proceso de gestión del riesgo**. El **contexto** incluye el ambiente interno y externo de la organización y el propósito de la actividad de **gestión del riesgo,** así como los antecedentes de los riesgos que se están evaluando.

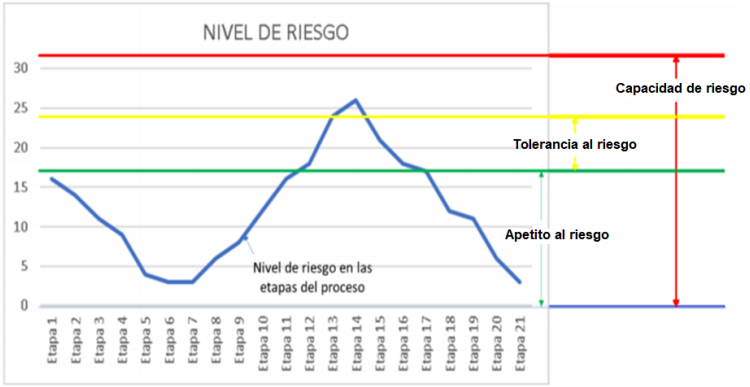
Al establecer el contexto, debemos tener en cuenta los objetivos de evaluación de riesgos, los criterios de riesgo, así como el programa de evaluación de riesgos.

Para una evaluación de riesgos, al establecer el contexto, deberíamos incluir su definición y la clasificación de los criterios de riesgo interno y externo:

Se pueden considerar entre otros factores como:

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: Ver conceptos básicos relacionados con el riesgo página

2. Apetito del riesgo: Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en cada una de las entidades, iniciando con las siguientes definiciones:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

2.1 Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

2.2 Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

2.3 Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

2.4 Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Determinación de la capacidad de riesgo: La entidad debe aplicar los valores de probabilidad e impacto contenidos en esta Guía y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

2.5 Determinación del apetito de riesgo: Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.

Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

2.6 Tolerancia de riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

3.1.2. PASO 2: IDENTIFICACIÓN DE RIESGOS:

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Se aplican las siguientes fases:

1. **Análisis de objetivos estratégicos y de los procesos:** Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

   Le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos

   La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

   Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico,

medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en ingles).

S	**Specific (Específicas):** Las metas deben ser escritas de manera simple y clara, logrando definir exactamente qué vamos a hacer. Específicas implica establecer el qué, el por qué y el cómo.
M	**Measurable (Medibles):** Para tener evidencia tangible de que se ha logrado un objetivo, es necesario que nuestras metas sean medibles, y por lo general, existe una meta final que engloba varias a corto plazo. En ciertas ocasiones será sencillo medir tu progreso, en el caso de metas monetarias como ahorros o inversiones, se podrá ver reflejado en tu cuenta de banco. En otros casos, el resultado se puede controlar a través de una bitácora o registro que muestre constantemente el progreso, sea semanal o mensual.
A	**Achievable (Alcanzables):** Las metas deben ser algo que puedas cumplir, para ello asegúrate que sea lo suficientemente retadora, pero bien definida para que puedas lograrla. Debes estar consiente que tienes los conocimientos, habilidades y competencias necesarios para cumplirlas, de lo contrario solito estarás complicándote a falta de recursos o experiencia.
R	**Realistic (Relevantes o Realista):** Las metas deben medir resultados, no actividades, es decir, cuando determines una meta, asegúrate de que sea realista y orientada a un resultado. También se denominan como orientadas a resultados, con el fin de seguir una serie de pasos que te lleven a un objetivo deseado. Determina los beneficios de alcanzar una meta.
T	**Timely (Calendarizadas):** Es necesario establecer un periodo límite para conseguir cada objetivo, denominando como urgentes aquellos que generen cierta tensión y presión entre la realidad actual y la visión de la meta. Sin dicha tensión, la meta conlleva pocas posibilidades de obtener resultados significativos.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

2. **Identificación de los puntos de riesgo:** Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017

3. **Identificación de áreas de impacto.** El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

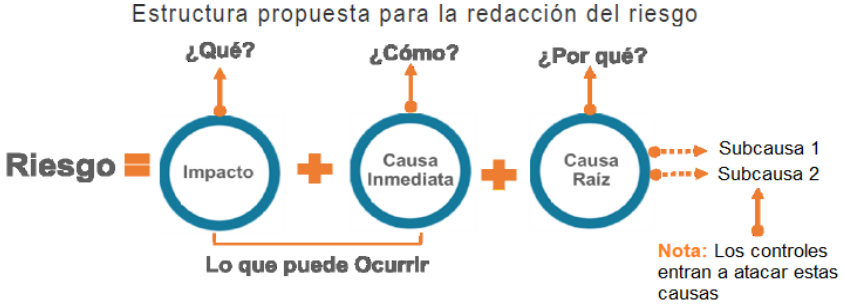
4. **Identificación de áreas de factores de riesgo:** Son las fuentes generadoras de riesgos. En la Tabla se encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

Factor	Definición	Descripción	Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos.	Infraestructura.	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Errores de grabación, autorización.			Incendios
		Errores en cálculos para pagos internos y externos.			Inundaciones
		Falta de capacitación, temas relacionados con el personal.			Daños a activos fijos
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	Hurto activos.	Evento externo.	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Posibles comportamientos no éticos de los empleados.			Asalto a la oficina
		Fraude interno (corrupción, soborno).			Atentado, vandalismo, orden público
Tecnología.	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos			Caída de redes
		Caída de aplicaciones			Errores en programas

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Los factores relacionados son una guía, se pueden analizar los que considere de acuerdo con la complejidad la entidad y el sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

5. **Descripción del riesgo:** la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase <u>POSIBILIDAD DE</u> y se analizan los siguientes aspectos:



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- ✓ **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- ✓ **Causa raíz:** Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para una adecuada redacción del riesgo.

- ✓ No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- ✓ No describir causas como riesgos. Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- ✓ No describir riesgos como la negación de un control. Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.
- ✓ No existen riesgos transversales, lo que pueden existir son causas transversales. Ejemplo: pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

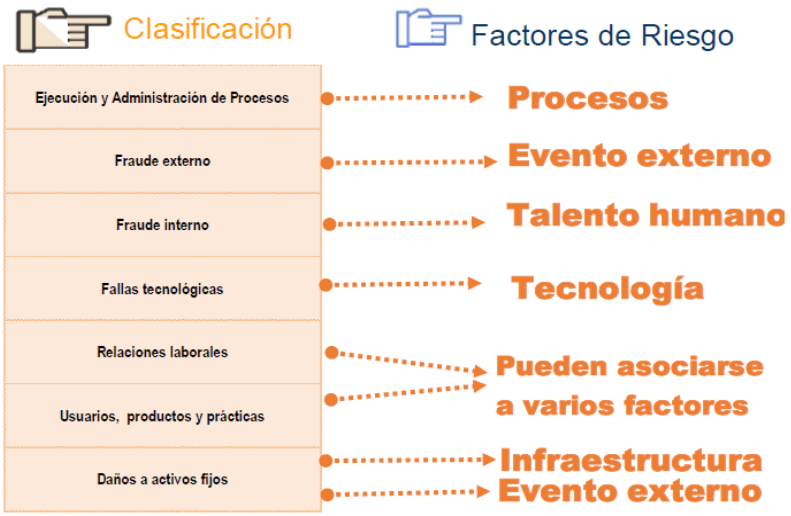
6. Clasificación del riesgo: Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías**:**

Ejecución y administración de procesos.	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo.	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno.	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas.	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales.	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas.	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos
Daños a activos fijos/ eventos externos.	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Teniendo en cuenta que en la Tabla anterior se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

3.1.3. PASO 3: VALORACIÓN DE RIESGO[7]:

Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente). La valoración del riesgo de desarrolla a través del análisis y la evolución del riesgo.

1. **Análisis de riesgos:** en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

   a) **Determinar la probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo.

[7] NTC ISO31000, Numerales 2.14, 2.15, 2.21, 2.24

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la **exposición al riesgo** del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividades relacionadas con la gestión en entidades públicas

Actividad.	Frecuencia de la Actividad.	Probabilidad frente al Riesgo.
Planeación estratégica.	1 vez al año.	Muy baja.
Actividades de talento humano, jurídica, administrativa.	Mensual.	Media.
Contabilidad, cartera.	Semanal.	Alta.
*Tecnología (incluye disponibilidad de aplicativos), tesorería. *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria.	Muy alta.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año,** en la tabla 4 se establecen los criterios para definir el nivel de probabilidad.

	Frecuencia de la actividad.	Probabilidad

Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	800%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

b) **Determinar el impacto:** Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel

insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.
Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

		Afectación Económica	Reputacional
Leve	20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

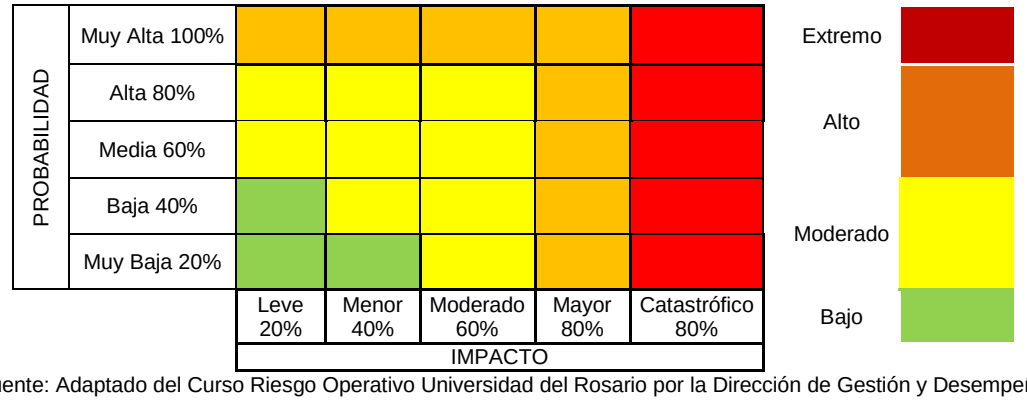
Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

3.1.4. PASO 4: EVALUACION DE RIESGO:

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

1. Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura 14).



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

2. **Valoración de controles:** en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

   a) La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
   b) Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

3. **Estructura para la descripción del control:** para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

   a) **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
   b) **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
   c) **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

4. **Tipología de controles y los procesos:** a través del ciclo de los procesos es posible establecer cuándo se activa un control y , por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura se consideran 3 fases globales del ciclo de un proceso así:

Entradas	Interrelaciones	Salidas
Recursos que requiere el proceso.	Actividades de permiten transformar las entradas en productos y/o servicios.	Recursos que requiere el proceso.
Controles Preventivos.	**Controles Detectivos.**	**Controles Correctivos.**
Va a las causas del riesgo. Atacan la probabilidad de ocurrencia del riesgo.	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.	Atacan el impacto frente a la materialización del riesgo.
Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.	Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.	Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

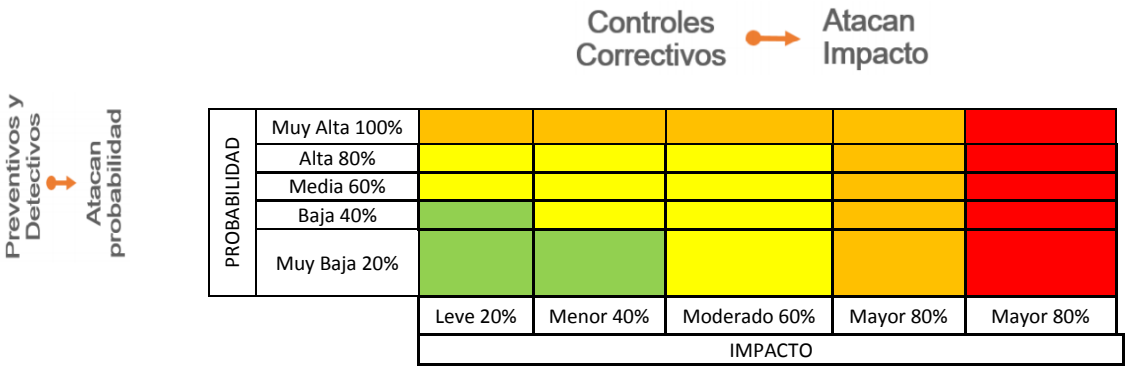
a. **Análisis y evaluación de los controles – Atributos:** A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar la descripción y peso asociados a cada uno así:

Características.			Descripción.	Peso.
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Implementación	Automático Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos *.	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso. -	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso . -	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

*. Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

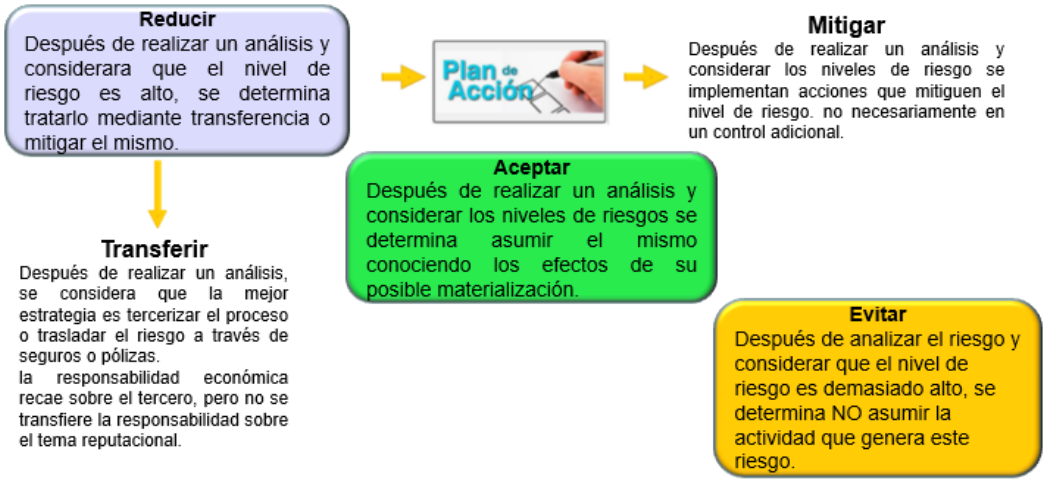
Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura 14 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



b. **Nivel de riesgo (riesgo residual):** es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

c. **Estrategias para combatir el riesgo:** decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.
Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

3.1.5. PASO 5: MONITOREO Y REVISIÓN:

El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

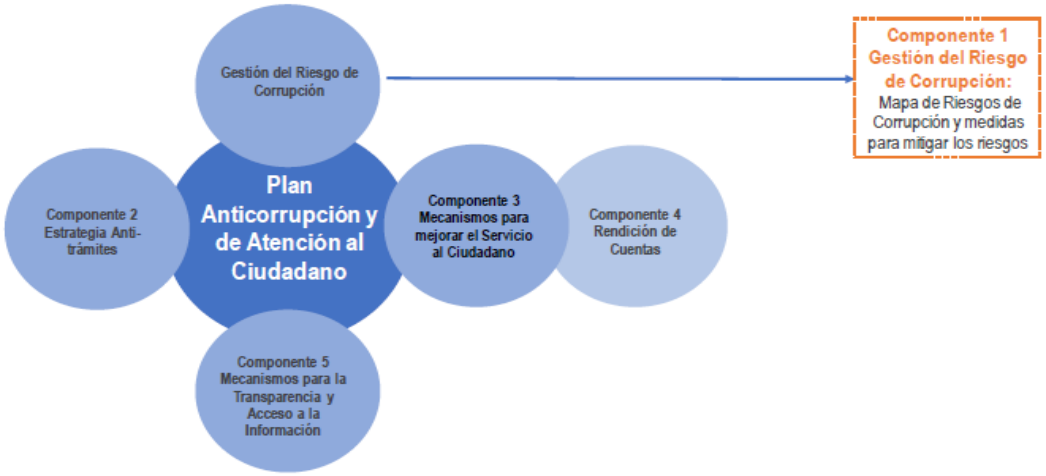
LENEA ESTRATEGICA
Define el marco para la gestión, el control y supervisa su cumplimiento, para que la entidad tenga un enfoque basado en riesgos y evaluarlos de forma sistemática en el marco del Comité Institucional de Coordinación de Control Interno. Está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

1ª. LÍNEA DE DEFENSA	2ª. LÍNEA DE DEFENSA	3ª. LÍNEA DE DEFENSA
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa

Corresponde a los servidores en sus diferentes niveles de la organización la aplicación de los controles tal como han sido diseñados, como parte del día a día y autocontrol de las actividades de la gestión a su cargo. Su Rol principal es diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.	Corresponde a la Media y Alta Gerencia, donde se incluyen las Oficinas Asesoras de Planeación o quienes hagan sus veces, los Líderes de Proceso, Coordinadores, supervisores o interventores de contratos o proyectos, comités de riesgos (donde existan) entre otros, es a quienes corresponde establecer mecanismos que les permitan ejecutar un seguimiento o autoevaluación permanente de la gestión, orientando y generando alertas a la 1a línea de defensa. Su rol principal es el de asegurar de que los controles y procesos de gestión del riesgo de la 1a línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo.	Corresponde a la Oficina de Control Interno o quien haga sus veces hacer el seguimiento objetivo e independiente de la gestión, utilizando los mecanismos y herramientas de auditoría interna, o bien estableciendo cursos de acción que le permitan generar alertas y recomendaciones a la administración, a fin de evitar posibles incumplimientos o materializaciones de riesgos en los diferentes ámbitos de la entidad. Su rol principal es el de proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento es a través de las auditorías internas que cubran todos los componentes del S.C.I.

3.2 MONITOREO DE RIESGOS DE CORRUPCIÓN.

La Ley 1474 de 2011 (artículo 73) estableció el marco del Plan Anticorrupción y de Atención al Ciudadano establecido y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: Gestión del riesgo de corrupción. Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción.



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2020.

Los riesgos asociados a posibles actos de corrupción, para la presente guía se consideran los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

3.2.1 GENERALIDADES ACERCA DE LOS RIESGOS DE CORRUPCIÓN

El Gerentes y los Líderes de los Procesos, junto con sus equipos de trabajo, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la Oficina asesora de Planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

- ✓ Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.
- ✓ Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.
- ✓ Ajustes y modificaciones: después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- ✓ Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- ✓ Seguimiento: el jefe de Control Interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

Teniendo en cuenta la criticidad del tema y que se requiere su publicación en página web, las entidades podrán anonimizar la información relacionada con los controles establecidos que pueden tener relación con información clasificada o reservada

Información Anonimizada								
No.	Riesgo	Clasificación	Casusa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control

1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros.	Corrupción	Falta de …	Probable	Catastrófico	Catastrófico	Evitar	Información Anonimizada

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2018

Se debe tener en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o un convenio internacional ratificado por el Congreso o la Constitución. Una resolución no puede clasificar la información como clasificada o reservada.

3.2.2 IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN.

3.2.2.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

A continuación, se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Direccionamiento estratégico (alta dirección)	✓ Concentración de autoridad o exceso de poder. Extralimitación de funciones. ✓ Ausencia de canales de comunicación. ✓ Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	✓ Inclusión de gastos no autorizados. ✓ Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. ✓ Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. ✓ Inexistencia de archivos contables. ✓ Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	✓ Estudios previos o de factibilidad deficientes. ✓ Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). ✓ Pliegos de condiciones hechos a la medida de una firma en particular. ✓ Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). ✓ Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. ✓ Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. ✓ Urgencia manifiesta inexistente. ✓ Concentrar las labores de supervisión en poco personal. ✓ Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	✓ Ausencia o debilidad de medidas y/o políticas de conflictos de interés.

	✓ Concentración de información de determinadas actividades o procesos en una persona. ✓ Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. ✓ Ocultar la información considerada pública para los usuarios. ✓ Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	✓ Inexistencia de canales de denuncia interna o externa. ✓ Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. ✓ Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. ✓ Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	✓ Cobros asociados al trámite. ✓ Influencia de tramitadores. ✓ Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	✓ Falta de procedimientos claros para el trámite. ✓ Imposibilitar el otorgamiento de una licencia o permiso. ✓ Tráfico de influencias: (amiguismo, persona influyente).

Fuente: Secretaría de Transparencia de la presidencia de la república, 2018.

3.2.3 LINEAMIENTOS PARA LA IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN.

Las preguntas clave para la identificación del riesgo son:

- ✓ ¿Qué puede suceder?
- ✓ ¿Cómo puede suceder?
- ✓ ¿Cuándo puede suceder?
- ✓ ¿Qué consecuencias tendría su materialización?

3.2.3.1 Descripción del riesgo de corrupción

RIESGO DE CORRUPCIÓN
Definición de riesgo de corrupción: 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. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder de incidencias en la toma de decisiones y la administración de los bienes públicos" (Conpes No 167 de 2013).
Es necesario que en la descripción del riesgo concurra los componentes de su definición, así ==> **ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACION DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO**.

Fuente: Secretaría de Transparencia de la presidencia de la república, 2018.

3.2.3.2 Matriz para la definición del riesgo de corrupción

MATRIZ: DEFINICÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo.	Acción u omisión.	Uso del poder.	Desviar la gestión de lo público.	Beneficio privado.
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros.	X	X	X	X

3.2.4 VALORACIÓN DEL RIESGO

3.2.4.1 La determinación de la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en el tratamiento para los riesgos de procesos en numeral 3.1.1 de esta guía. Es importante resaltar que la frecuencia a la que se hace referencia en 3.1.1 se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo, en este sentido, y para este análisis, se retoma la tabla definida en el aparte 3.1.1 de la presente guía:

	Frecuencia de la actividad.	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	800%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

3.2.4.2 La determinación del impacto.

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles: i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos de procesos.

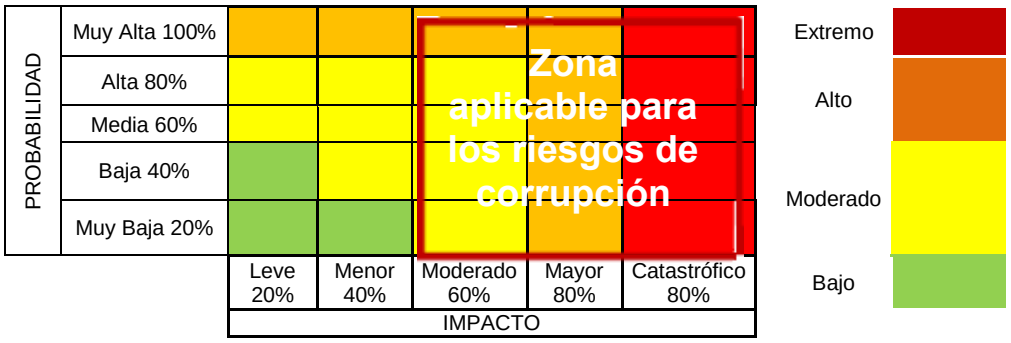
Ahora bien, para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente al riesgo identificado:

No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA.	RESPUESTAS SI = 1 NO = 0
1	¿Afectar al grupo de funcionarios del proceso?	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	
3	¿Afectar el cumplimiento de misión de la Entidad?	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?	
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?	

6	¿Generar pérdida de recursos económicos?	
7	¿Afectar la generación de los productos o la prestación de servicios?	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?	
9	¿Generar pérdida de información de la Entidad?	
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?	
11	¿Dar lugar a procesos sancionatorios?	
12	¿Dar lugar a procesos disciplinarios?	
13	¿Dar lugar a procesos fiscales?	
14	¿Dar lugar a procesos penales?	
15	¿Generar pérdida de credibilidad del sector?	
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas? (**Nota:** Si la respuesta a la pregunta es afirmativa, el riesgo se considera catastrófico).	
17	¿Afectar la imagen regional?	
18	¿Afectar la imagen nacional?	
• Responder afirmativamente de UNA a CINCO preguntas genera un impacto Moderado. **MODERADO:** Genera medianas consecuencias sobre la entidad.		
• Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor. **MAYOR:** Genera altas consecuencias sobre la entidad.		
• Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto Catastrófico		

3.2.4.3 Análisis preliminar (riesgo inherente):

En esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor establecida en el numeral 4.1 de la presente guía, teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimitan como se muestra a continuación:



3.2.4.4 Valoración de controles.

La valoración de los controles existentes establecido en el numeral 4.2, así como las demás disposiciones contenidas en el paso 4 de esta guía, son aplicables a la gestión del riesgo de corrupción.

3.3 SEGURIDAD DE LA INFORMACIÓN.

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)[8], el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

3.3.1 RESPONSABLE DE SEGURIDAD DIGITAL

Cada entidad pública debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

- ✓ Definir el procedimiento para la Identificación y Valoración de Activos.
- ✓ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- ✓ Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- ✓ Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- ✓ Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

3.3.2 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN.

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, (Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

[8] Tomado de: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad

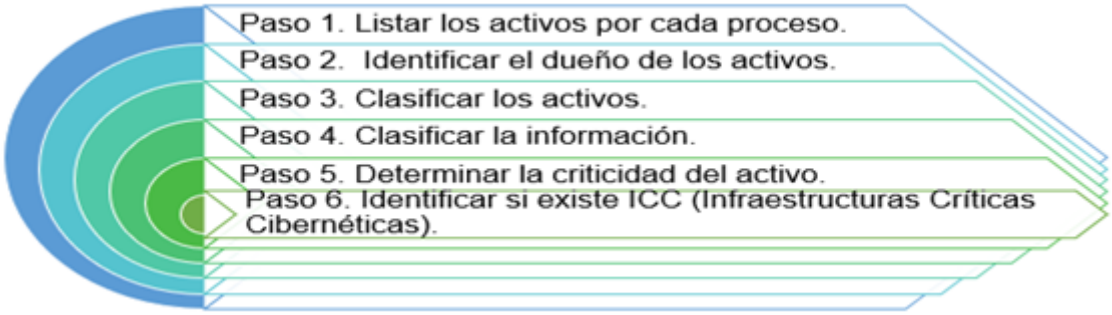
Es necesario que la entidad pública identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

Activos

1. **Equipos.** Hace referencia a activos de hardware y software que pertenecen y pueden ser afectados en el sistema	4 **Personas.** Los activos de este grupo hacen referencia a labores que realizan personas que pueden ser afectados en el sistema	5 **Datos e Información.** Los activos de este grupo son los más delicados y vulnerables en la matriz de riesgos, porque son los que van a almacenar y manejar la información que es obtenida por los GPS y otros medios de información
Programas de comunicación	Informática/soporte Interno	Correo electrónico
Programas de Producción de datos	Soporte Técnico Externo	Bases de datos internos
Portátiles	Servicio de Limpieza de Planta	Bases de datos externos
Computadoras	Servicio de Limpieza Externo	Página Web interna (Intranet) Respaldos
Servidores		Infraestructura (Planes, Documentación, etc.)
Cortafuegos		Informática (Planes, Documentación, etc.)
Equipos de Red Inalámbrica		Sistemas de autenticación DA, LDAP
Equipos de red cableada		Sistemas de información no institucionales Navegación en Internet

¿COMO IDENTIFICAR LOS ACTIVOS?:



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Paso 1. Listar los activos por cada proceso: En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Ejemplo: Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Las entidades públicas pueden adicionar identificadores o nemónicos para complementar la identificación de los activos.

Paso 2. Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

PROCESO	ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad	Jefe Oficina de Nómina
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Generalmente el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

Paso 3. Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.

Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

PROCESO	ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO	TIPO DE ACTIVO
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina	Información
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad	Jefe Oficina de Nómina	Software
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina	Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 4. Clasificar la información: Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

PROCESO	ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina	Información	Información Reservada	No Contiene datos personales
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad	Jefe Oficina de Nómina	Software	N/A	N/A
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina	Información	Información Pública	No contiene datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Al realizar la identificación del contexto externo, la entidad pública debería tener

plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas, sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios a tener en cuenta respecto a la información. El área jurídica de la entidad debe colaborar en esta tarea específica.

Paso 5. Determinar la criticidad del activo (Valoración del Activo): Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia la Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información (MSPI)[9] , estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

PROCESO	ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina	Información	Información Reservada	No Contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad	Jefe Oficina de Nómina	Software	N/A	N/A	BAJA	MEDIA	BAJA	BAJA
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina	Información	Información Pública	No contiene datos	BAJA	MEDIA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

[9] 5 http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guía #5 Gestión Clasificación de Activos

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICCS: Se invita a que las entidades públicas identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$ 464.619.736	3 años en recuperación

Fuente: Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia. Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición

Si la entidad pública determina que tiene ICC, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

3.3.3. VALORACIÓN DEL RIESGO.

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en el tratamiento para los riesgos de procesos en numeral 3.1.1 de esta guía. Es importante resaltar que la frecuencia a la que se hace referencia en 3.1.1 se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo, en este sentido, y para este análisis, se retoma la tabla definida en el aparte 3.1.1 de la presente guía:

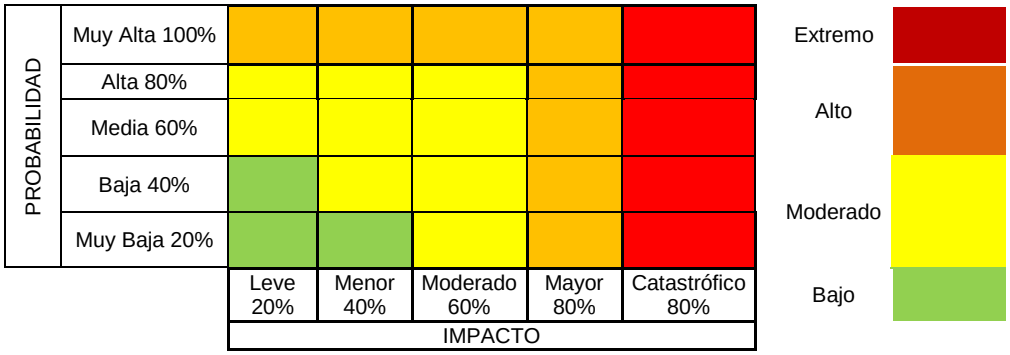
	Frecuencia de la actividad.	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	800%

Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

		Afectación Económica	Reputacional
Leve	20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 4.1 de la presente guía, que se retoma a continuación:



3.3.4. IDENTIFICAR LOS RIESGOS INHERENTES DE SEGURIDAD DIGITAL

Como lo indica el numeral 5.2 de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Identificación del riesgo en entidades Públicas” emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- ✓ Pérdida de la confidencialidad.
- ✓ Pérdida de la integridad.

- ✓ Pérdida de la disponibilidad.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

3.3.5. IDENTIFICACIÓN DE AMENAZAS.

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D), fortuito (F) o ambientales (A)

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal.	Reto. Ego	Piratería. Ingeniería social
Criminal de la computación.	Destrucción de la información. Divulgación ilegal de la información.	Crimen por computador. Acto fraudulento
Terrorismo.	Chantaje. Destrucción.	Ataques contra el sistema. DDoS. Penetración en el sistema.
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses).	Ventaja competitiva. Espionaje económico.	Ventaja de defensa. Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos).	Curiosidad. Ganancia monetaria	Asalto a un empleado. Chantaje.

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección

	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita

3.3.6. IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES EXISTENTES.

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

3.3.7. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL.

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP: Evitar, aceptar, compartir o mitigar el riesgo.

Si la entidad pública decide mitigar o tratar el riesgo mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad digital, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo

3.3.8. PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL E INDICADORES PARA LA GESTIÓN DEL RIESGO.

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos, de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" emitida por el DAFP.

3.3.9. CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN.

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

Procedimientos operacionales y responsabilidades.	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
Procedimientos de operación documentados.	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios.	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Gestión de capacidad.	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación.	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos.	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos.	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo.	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información.	Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

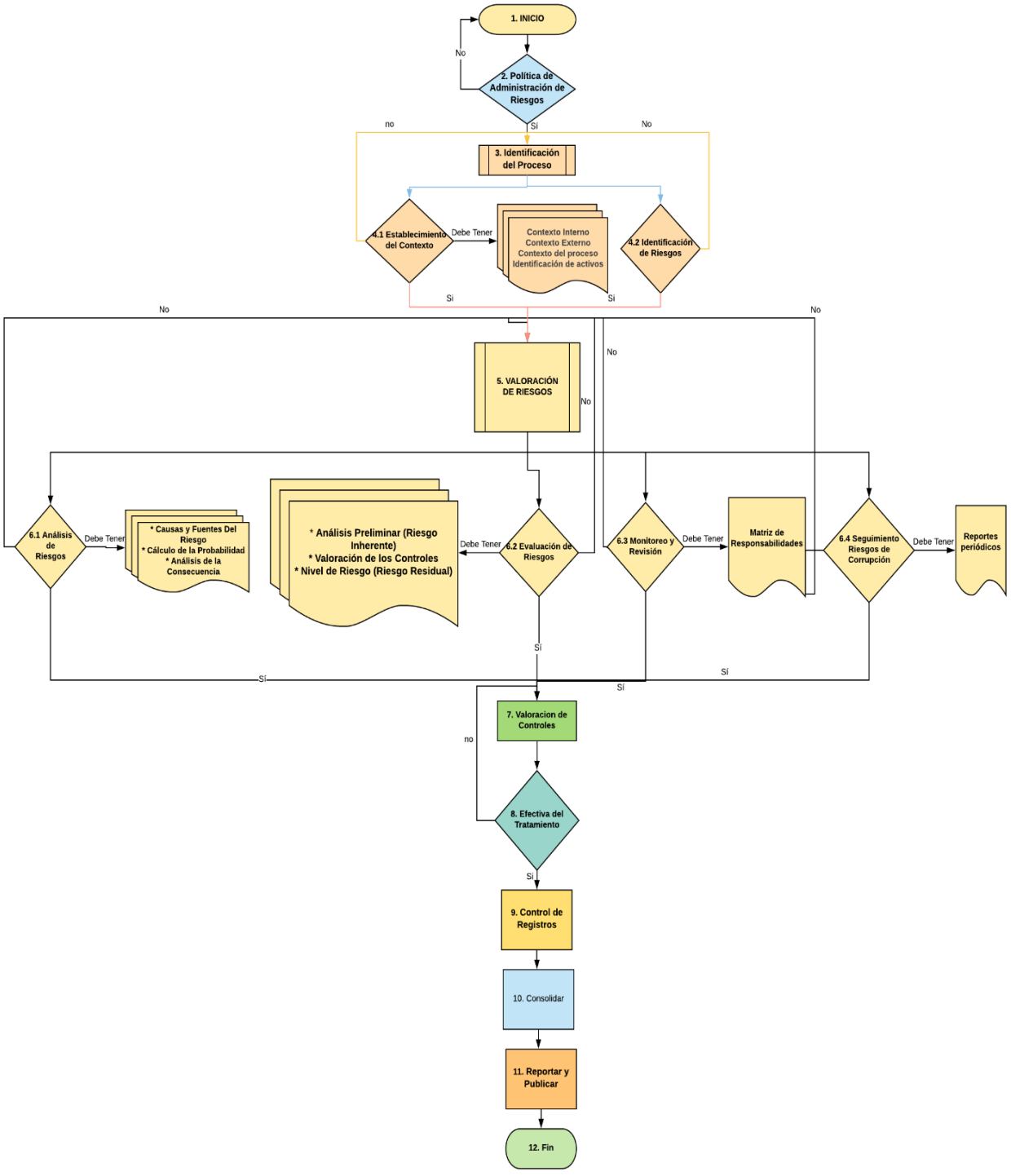
3.3.10. CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad digital empleando los siguientes controles, tomados del Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen, siempre y cuando se ajusten al análisis de riesgos.
El contenido de la tabla se describe en el numeral 5 de la presente guía.

4. FLUJOGRAMA

PROCEDIMIENTO		ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES - RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL.				
No	ACTIVIDAD	QUE	QUIEN	CUANDO	DONDE	COMO
1	Ver flujograma	Inicio.				
2		Política de Administración de Riesgos.	Gerente	Según lo establecido en la normatividad vigente.	Transversal a todos los procesos.	Declaración.
3		Identificación del Proceso	Líder de Proceso.	Al momento de iniciar la revisión de los riesgos o cuando se requiera	Nivel Central o Centros de Atención.	Análisis documentación del proceso.
4		Establecimiento del Contexto	Líder de Proceso.	Durante el análisis documentación del proceso a elaborar o revisar	Nivel Central o Centros de Atención.	FR-GQ 05.
5		Identificación de Riesgos	Líder de Proceso.		Nivel Central o Centros de Atención.	FR-GQ 06 de gestión FR-GQ 14 Digital

6		Identificación controles	Líder de Proceso.	Durante el análisis del documento a elaborar o revisar	Nivel Central o Centros de Atención.	FR-GQ 07 de gestión FR-GQ 15 Digital
7		Evaluación de controles.	Líder de Proceso.		Nivel Central o Centros de Atención.	FR-GQ 08
8		Evaluación de Riesgos	Líder de Proceso.		Nivel Central o Centros de Atención.	FR-GQ 09
9		Monitoreo y Revisión	Líder de Proceso.		Nivel Central o Centros de Atención.	FR-GQ 09
10		Seguimiento Riesgos de Corrupción	Líder de Proceso Nivel Central.	Revisiones periódicas por el líder del proceso.	Nivel Central	FR-GQ-51
11		Impacto de Corrupción	Líder de Proceso Nivel Central.			FR-GQ-51
12		Consolidar	Planeación	Luego de la elaboración de riesgos	Oficina Asesora de Planeación.	FR-GQ-10
13		Reportar y Publicar	Planeación		Oficina Asesora de planeación.	FR-GQ-09 FR-GQ-16 FR-GQ-51
14		Fin.				


1. INICIO
No
2. Política de Administración de Riesgos
Si
no
No
3. Identificación del Proceso
4.1 Establecimiento del Contexto
Debe Tener
Contexto Interno
Contexto Externo
Contexto del proceso
Identificación de activos
4.2 Identificación de Riesgos
Si
Si
No
No
5. VALORACIÓN DE RIESGOS
No
No
6.1 Análisis de Riesgos
Debe Tener
* Causas y Fuentes Del Riesgo
* Cálculo de la Probabilidad
* Análisis de la Consecuencia
* Análisis Preliminar (Riesgo Inherente)
* Valoración de los Controles
* Nivel de Riesgo (Riesgo Residual)
Debe Tener
6.2 Evaluación de Riesgos
6.3 Monitoreo y Revisión
Debe Tener
Matriz de Responsabilidades
6.4 Seguimiento Riesgos de Corrupción
Debe Tener
Reportes periódicos
Sí
Sí
Sí
Sí
7. Valoracion de Controles
no
8. Efectiva del Tratamiento
Sí
9. Control de Registros
10. Consolidar
11. Reportar y Publicar
12. Fin

5. ANEXO

5.1. ANEXO A DE LA NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001

5.1.1. OBJETIVOS DE CONTROL Y CONTROLES

1. INTRODUCCIÓN

Los objetivos de control y los controles enumerados en la Tabla A.1 se han obtenido directamente de los de la NTC-ISO/IEC 17799:2005, numerales 5 a 15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales. Los objetivos de control y controles de estas tablas se deben seleccionar como parte del proceso de SGSI especificado en el numeral 4.2.1.

La norma NTC- ISO/IEC 17799:2005, numerales 5 a 15, proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados en el literal A.5 a A.15.

A.X – Dominio
A.X.X – Objetivo de Control
A.X.X.X - Controles

Tabla A.1. Objetivos de control y controles

A.5 POLÍTICA DE SEGURIDAD		
A.5.1 Política de seguridad de la información. **Objetivo:** Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.		
A.5.1.1	Documento de la política de seguridad de la información.	**Control:** La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.
A.5.1.2	Revisión de la política de seguridad de la información.	**Control:** La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización interna. **Objetivo:** gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la dirección con la seguridad de la información.	La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	**Control:** Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.

A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	**Control:** Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	**Control:** Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.
A.6.1.5	Acuerdos sobre confidencialidad	**Control.** Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con las autoridades	**Control:** Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos de interés especiales	**Control:** Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información.	**Control.** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.
A.6.2 Partes externas. **Objetivo:** mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.		
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	**Control:** Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	**Control:** Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	**Control:** Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad
A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad por los activos. **Objetivo:** lograr y mantener la protección adecuada de los activos organizacionales		
A.7.1.1	Inventario de activos	**Control:** Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.

A.7.1.2	Propiedad de los activos	**Control:** Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"[10] de una parte designada de la organización.
A.7.1.3	Uso aceptable de los activos	**Control:** Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.
A.7.2 Clasificación de la información. **Objetivo:** asegurar que la información recibe el nivel de protección adecuado.		
A.7.2.1	Directrices de clasificación	**Control:** La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
A.7.2.2	Etiquetado y manejo de información	**Control:** Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.8.1 Antes de la contratación laboral[11] **Objetivo:** asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.		
A.8.1.1	Roles y responsabilidades	**Control:** Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.
A.8.1.2	Selección	**Control:** Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos
A.8.1.3	Términos y condiciones laborales.	**Control:** Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.
A.8.2 Durante la vigencia de la contratación laboral. **Objetivo:** asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.		

[10] El término "propietario" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

[11] Explicación: La palabra “contratación laboral" cubre todas las siguientes situaciones: empleo de personas (temporal o a término indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos acuerdos.

A.8.2.1	Responsabilidades de la dirección	**Control:** La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	**Control:** Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.
A.8.2.3	Proceso disciplinario	**Control:** Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.
A.8.3 Terminación o cambio de la contratación laboral. **Objetivo**: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.		
A.8.3.1	Responsabilidades en la terminación	**Control:** Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.
A.8.3.2	Devolución de activos	**Control:** Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.
A.8.3.3	Retiro de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.9.1 Áreas seguras. **Objetivo:** evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización		
A.9.1.1	Perímetro de seguridad física	**Control:** Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información
A.9.1.2	Controles de acceso físico.	**Control:** Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	**Control:** Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A.9.1.4	Protección contra amenazas externas y ambientales.	**Control:** Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.
A.9.1.5	Trabajo en áreas seguras.	**Control:** Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las

		instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.
A.9.2 Seguridad de los equipos. **Objetivo:** evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección de los equipos.	**Control:** Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado
A.9.2.2	Servicios de suministro	**Control:** Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.
A.9.2.3	Seguridad del cableado.	**Control:** El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.
A.9.2.4	Mantenimiento de los equipos.	**Control:** Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	**Control:** Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos.	**Control:** Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.
A.9.2.7	Retiro de activos	**Control** Ningún equipo, información ni software se deben retirar sin autorización previa.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A.10.1 Procedimientos operacionales y responsabilidades. **Objetivo:** asegurar la operación correcta y segura de los servicios de procesamiento de información.		
A.10.1.1	Documentación de los procedimientos de operación	**Control:** Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
A.10.1.2	Gestión del cambio.	**Control:** Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.
A.10.1.3	Distribución de funciones.	**Control:** Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	**Control:** Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.
A.10.2 Gestión de la prestación del servicio por terceras partes. **Objetivo:** implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.		
A.10.2.1	Prestación del servicio	**Control:** Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio

		incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	**Control:** Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	**Control:** Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.
A.10.3 Planificación y aceptación del sistema. **Objetivo:** minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	Gestión de la capacidad.	**Control:** Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.
A.10.3.2	Aceptación del sistema.	**Control:** Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A.10.4 Protección contra códigos maliciosos y móviles. **Objetivo:** proteger la integridad del software y de la información.		
A.10.4.1	Controles contra códigos maliciosos.	**Control:** Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.
A.10.4.2	Controles contra códigos móviles.	**Control:** Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.
A.10.5 Respaldo. Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de la información.		
A.10.5.1	Respaldo de la información.	**Control:** Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
A.10.6 Gestión de la seguridad de las redes. **Objetivo:** asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de las redes.	**Control:** Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de la red.	**Control:** En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.

A.10.7 Manejo de los medios. **Objetivo:** evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.		
A.10.7.1	Gestión de los medios removibles	**Control:** Se deben establecer procedimientos para la gestión de los medios removibles
A.10.7.2	Eliminación de los medios.	**Control:** Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.
A.10.7.3	Procedimientos para el manejo de la información.	**Control:** Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.
A.10.7.4	Seguridad de la documentación del sistema.	**Control:** La documentación del sistema debe estar protegida contra el acceso no autorizado.
A.10.8 Intercambio de la información. **Objetivo:** mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.		
A.10.8.1	Políticas y procedimientos para el intercambio de información	**Control** Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.
A.10.8.2	Acuerdos para el intercambio	**Control** Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.
A.10.8.3	Medios físicos en tránsito.	**Control** Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.
A.10.8.4	Mensajería electrónica.	**Control** La información contenida en la mensajería electrónica debe tener la protección adecuada
A.10.8.5	Sistemas de información del negocio.	**Control** Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.
A.10.9 Servicios de comercio electrónico. **Objetivo:** garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.		
A.10.9.1	Comercio electrónico	**Control:** La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.
A.10.9.2	Transacciones en línea	**Control:** La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.
A.10.9.3	Información disponible al público	**Control:** La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.
A.10.10 Monitoreo. Objetivo: detectar actividades de procesamiento de la información no autorizadas.		

A.10.10.1	Registro de auditorías	**Control:** Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.
A.10.10.2	Monitoreo del uso del sistema	**Control:** Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad
A.10.10.3	Protección de la información del registro	**Control:** Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
A.10.10.4	Registros del administrador y del operador	**Control:** Se deben registrar las actividades tanto del operador como del administrador del sistema.
A.10.10.5	Registro de fallas	**Control:** Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.
A.11 CONTROL DE ACCESO		
A.11.1 Requisito del negocio para el control de acceso. **Objetivo:** controlar el acceso a la información.		
A.11.1.1	Política de control de acceso	**Control:** Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.
A.11.2 Gestión del acceso de usuarios. Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.		
A.11.2.1	Registro de usuarios.	**Control:** Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios.	Control Se debe restringir y controlar la asignación y uso de privilegios.
A.11.2.3	Gestión de contraseñas para usuarios.	**Control:** La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	**Control:** La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.
A.11.3 Responsabilidades de los usuarios. Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.		
A.11.3.1	Uso de contraseñas.	**Control:** Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.
A.11.3.2	Equipo de usuario desatendido.	**Control:** Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.3.3	Política de escritorio despejado y de pantalla despejada	**Control:** Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.
A.11.4 Control de acceso a las redes. Objetivo: evitar el acceso no autorizado a servicios en red.		

A.11.4.1	Política de uso de los servicios de red.	**Control:** Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.
A.11.4.2	Autenticación de usuarios para conexiones externas.	**Control:** Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación de los equipos en las redes.	Control La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	**Control:** El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado
A.11.4.5	Separación en las redes.	**Control:** En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.
A.11.4.6	Control de conexión a las redes.	**Control:** Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).
A.11.4.7	Control de enrutamiento en la red.	**Control:** Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.
A.11.5 Control de acceso al sistema operativo.		
Objetivo: evitar el acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de ingreso seguros	**Control:** El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.
A.11.5.2	Identificación y autenticación de usuarios.	**Control:** Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.
A.11.5.3	Sistema de gestión de contraseñas.	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.11.5.4	Uso de las utilidades del sistema	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.
A.11.5.5	Tiempo de inactividad de la sesión	**Control:** Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.
A.11.5.6	Limitación del tiempo de conexión.	**Control:** Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo
A.11.6 Control de acceso a las aplicaciones y a la información. Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.		
A.11.6.1	Restricción de acceso a la información.	**Control:** Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con a política definida de control de acceso.
A.11.6.2	Aislamiento de sistemas sensibles.	**Control:** Los sistemas sensibles deben tener un entorno informático dedicado (aislados).
A.11.7 Computación móvil y trabajo remoto. Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.		

A.11.7.1	Computación y comunicaciones móviles.	**Control:** Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.
A.11.7.2	Trabajo remoto.	**Control:** Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
A.12.1 Requisitos de seguridad de los sistemas de información. Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requisitos de seguridad	**Control:** Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones. Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.		
A.12.2.1	Validación de los datos de entrada.	**Control:** Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados
A.12.2.2	Control de procesamiento interno.	**Control:** Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje.	**Control:** Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
A.12.2.4	Validación de los datos de salida.	**Control:** Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias
A.12.3 Controles criptográficos. Objetivo: proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos.	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión de llaves.	**Control:** Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.
A.12.4 Seguridad de los archivos del sistema. Objetivo: garantizar la seguridad de los archivos del sistema.		
A.12.4.1	Control del software operativo.	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.4.2	Protección de los datos de prueba del sistema.	**Control:** Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse
A.12.4.3	Control de acceso al código fuente de los programas	**Control:** Se debe restringir el acceso al código fuente de los programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte. Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.		

A.12.5.1	Procedimientos de control de cambios.	**Control:** Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	**Control:** Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.
A.12.5.3	Restricciones en los cambios a los paquetes de software.	**Control:** Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.12.5.4	Fuga de información	**Control:** Se deben evitar las oportunidades para que se produzca fuga de información.
A.12.5.5	Desarrollo de software contratado externamente	**Control:** La organización debe supervisar y monitorear el desarrollo de software contratado externamente.
A.12.6 Gestión de la vulnerabilidad técnica. Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	**Control:** Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información. Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.		
A.13.1.1	Reporte sobre los eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
A.13.1.2	Reporte sobre las debilidades de la seguridad	**Control:** Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	**Control:** Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	**Control:** Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.
A.13.2.3	Recolección de evidencia	**Control:** Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		

A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.		
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	**Control:** Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	continuidad del negocio y evaluación de riesgos	**Control:** Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	**Control:** Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.
A.14.1.4	Estructura para la planificación de la continuidad del negocio	**Control:** Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	**Control:** Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.
A.15 CUMPLIMIENTO		
A.15.1 Cumplimiento de los requisitos legales. Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.		
A.15.1.1	Identificación de la legislación aplicable.	**Control:** Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización
A.15.1.2	Derechos de propiedad intelectual (DPI).	**Control:** Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
A.1.5.1.3	Protección de los registros de la organización.	**Control:** Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.
A.15.1.4	Protección de los datos y privacidad de la información personal.	**Control:** Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	**Control:** Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

A.15.1.6	Reglamentación de los controles criptográficos.	**Control:** Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico Objetivo: asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.		
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	**Control:** Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.
A.15.2.2	Verificación del cumplimiento técnico.	**Control:** Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.

6. TERMINOS Y DEFINICIONES

- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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 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 inherente**: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Gestión del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Confidencialidad: P**ropiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Vulnerabilidad: E**s una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Integridad: P**ropiedad de exactitud y completitud.
- **Tolerancia al riesgo:** Son los 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.
- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Control:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

7. REGISTRO DE CALIDAD:

Nombre formato	Código	Proceso	Responsable del Almacenamiento	Tiempo de Retención	Disposición Final
Contexto.	FR-GQ 05	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Identificación de riesgos de Gestión	FR-GQ 06	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Identificación de los controles	FR-GQ 07	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Evaluación de los controles	FR-GQ 08	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Mapa Riesgos de Gestión	FR-GQ 09	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Mapa de riesgos de proceso institucional	FR-GQ-10	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Listado de Activos Institucionales	FR-GQ 13	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación
Identificación Riesgos Digitales	FR-GQ 14	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación.

Calificación y Evaluación Riesgos Digitales	FR-GQ 15	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación.
Mapa Riesgos Digitales	FR-GQ 16	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación.
Mapa de riesgos de corrupción	FR-GQ-51	Oficina Asesora de Planeación	Oficina de planeación	2 años después de su actualización	Eliminación.

8. NORMATIVIDAD

- Ley 87 de 1993, “Por la cual se establecen normas para el ejercicio del control interno en la entidades y organismos del estado y se dictan otras disposiciones”.
- Ley 1753 de 2015, Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país".
- Decreto 1537 de 2001, “Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado”.
- Decreto 943 de 2014, “Por el Cual se actualiza el Modelo Estándar de Control Interno MECI”.
- Decreto 124 de 2016, “Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al “Plan Anticorrupción y de Atención al Ciudadano”.
- Decreto 1499 de 2017, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- NTC-ISO31000_Gestion_del_riesgo.
- Celis, Ó. B. (2012). Gestión Integral de Riesgos. Bogotá D.C.: Consorcio Gráfico Ltda.
- COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants.
- COSO Committee of Sponsoring Organizations of the Treadway Commission. PwC. Instituto de Auditores Internos de España. (2013). Control Interno - Marco Integrado. Marco y Apéndices. Instituto de Auditores Internos de España.
- ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
- ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
- ICONTEC Internacional. (2013). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL

RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

- Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C.
- Núñez, A. C. (9 de 11 de 2016). Inboundlead Blog. Obtenido de Los 7 Mejores Ejemplos de Objetivos SMART: https://blog.inboundlead.com/los-7-mejores-ejemplos-de-objetivos-smart-o-inteligentes-para-empresas.

9. BIBLIOGRAFIA

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (versión 5), del Departamento Administrativo de la Función Pública.

10. CONTROLES

La Oficina Asesora de Planeación, le hará seguimiento al cumplimiento de la Política para la Administración del Riesgo y el Diseño de Controles - Riesgos de Gestión, Corrupción y Seguridad Digital dentro de los tiempos establecidos para el monitoreo de los riesgos en los formatos:

Formato Código FR-GQ-06 “Mapa Riesgos de Gestión por Proceso”.
Formato Código FR-GQ-51 “Mapa de Riesgo de Corrupción”.

Lo anterior no será óbice para que la oficina de Planeación solicite información a algún proceso sobre la aplicación de sus controles.

CONTROL DE CAMBIOS

Versión No	Descripción u Origen del Cambio	Aprobó	Fecha
1	Se crea documento donde se establecer metodología para la correcta identificación, análisis, valoración y administración de riesgos de gestión, de corrupción y de seguridad digital.	Gerencia	2018/12/28
2	Se actualiza documento de acuerdo con los lineamientos establecidos por la función Públicas en: la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020.	Gerencia	2021/06/25