MANUAL- POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

AGENCIA DE RENOVACIÓN DEL TERRITORIO - ART

OFICINA DE PLANEACIÓN

Bogotá D.C.

Septiembre

2020

JUAN CARLOS ZAMBRANO ARCINIEGAS
Director General Agencia de Renovación del Territorio

ANDREA PAOLA FERNÁNDEZ GUARÍN
Jefe Oficina de Planeación

CARLOS ANDRÉS BALLESTEROS
Asesor TIC Dirección General

FREDY ALEJANDRO AGUAS
Profesional-Contratista
Dirección General

ISABEL PARRA BELLO
Profesional-Contratista
Oficina de Planeación

TABLA DE CONTENIDO

INTRODUCCIÓN

La Agencia de Renovación del Territorio-ART, a través del presente manual establece la política y las directrices para la adecuada administración de riesgos y define la metodología para la identificación, análisis, valoración, establecimiento de controles, tratamiento y seguimiento de los riesgos inherentes a los procesos, relacionados con los riesgos de gestión, de corrupción y de seguridad digital, con el propósito de evitar que interfieran en el cumplimiento de los objetivos y misión institucional.

El Comité Directivo, en sesión del 15 de diciembre de 2017 aprobó y adoptó el Manual Política de Administración de Riesgos para la ART; teniendo en cuenta que el Departamento Administrativo de la Función Pública-DAFP, modificó la metodología para la Gestión de Riesgos para las entidades públicas, el Comité Institucional de Coordinación de Control Interno de la Agencia, en sesión del 20 de agosto de 2019, aprobó la adecuación de la política y metodología y adoptó la política de administración de riesgos, conforme a la metodología del DAFP.

Como parte integral de la gestión de riesgos de la ART, se hace necesario incluir los riesgos de seguridad digital, los cuales hacen parte de la estrategia de gobierno digital para la implementación de un modelo de seguridad y privacidad de la información – MPSI en las entidades públicas que permita a la ART su correcto desempeño dentro de la política pública y resguardando su información de cualquier tipo de alteración, mal uso o perdida, así como permitir la toma de decisiones.

La administración de riesgos de la ART, se enmarca en lo dispuesto en el artículo 2.2.23.2 del Decreto 1499 de 2017, el cual actualiza del Modelo Estándar de Control Interno, a través del Manual Operativo del Modelo Integrado de Planeación y Gestión- MIPG, el artículo 4º del Decreto 1537 de 2001 el cual determina que la administración del riesgo, es parte integral del fortalecimiento del Sistema de Control Interno en las entidades públicas y define que las autoridades correspondientes, deberán establecer y aplicar políticas para su gestión; y el CONPES 3854 del 11 de abril de 2016, el cual establece la Política Nacional de Seguridad Digital que permite fortalecer las capacidades de la entidades públicas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

La Entidad, contempla la Gestión del Riesgo como parte de la implementación del Modelo Integrado de Planeación y Gestión-MIPG, el cual establece la gestión del riesgo en las Políticas de: Planeación Institucional, la cual hace énfasis en la formulación de la Política de Administración de Riesgos; Política de Seguridad Digital, que define los aspectos a tener en cuenta para asegurar los activos de información de las entidades públicas y la Política de Control Interno, la cual establece en el Modelo Estándar de Control Interno-MECI, las responsabilidades de las diferentes instancias de las Entidades, conforme a las tres líneas de defensa.

La Agencia de Renovación del Territorio - ART, adopta y ajusta la metodología para la Administración de Riesgos, de acuerdo con los estándares establecidos por el Departamento Administrativo de la Función Pública en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital” y sus anexos.

La Política de Administración de Riesgos de la ART, se establece a través del presente Manual y es aplicable a todos los niveles, procesos y servidores de la Entidad, como herramienta para el manejo y control de los riesgos, para asegurar el cumplimiento de los objetivos institucionales.

1. OBJETIVO

El Manual de Administración de Riesgo de la Agencia de Renovación del Territorio-ART, tiene como objetivo establecer los lineamientos, para la adecuada gestión de los riesgos, a los que está expuesto la Entidad en el marco de sus actuaciones y controlar las situaciones adversas que puedan impactar el cumplimiento de los objetivos y misión institucional.

2. ALCANCE

Los lineamientos acá presentados serán de aplicación obligatoria a todos los niveles y procesos de la ART, para los servidores públicos y contratistas, que presten sus servicios en la Entidad.

Inicia con el establecimiento de la Política de Administración de Riesgos, continúa con la identificación, análisis, valoración y tratamiento de estos, hasta el control, monitoreo y seguimiento de los riesgos. Para los riesgos de seguridad digital, una vez se cuenta con el establecimiento de la Política, se continúa con la identificación de activos de información y el catálogo de amenazas y vulnerabilidades, el análisis de riesgos de seguridad digital, valoración y tratamiento de estos, hasta el control, monitoreo y seguimiento de los riesgos, en pro del mantenimiento del Sistema de Gestión y la consecución de los objetivos y misión institucional.

3. MARCO NORMATIVO

Artículo 2º, literal a, de la Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.

Ley 1474 de 2011. Estatuto Anticorrupción.

Ley 1712 de 2014. Ley de transparencia y acceso a la información pública.

Decreto 1081 de 2015. Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Decreto 1083 de 2015, artículo 2.2.21.5.4 Administración de riesgos**.**

Decreto 1499 de 2017. Actualiza el Modelo Estándar de Control Interno –MECI.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital" y anexos. V.4. octubre de 2018. Departamento Administrativo de la Función Pública.

ANEXO 4 Guía para la administración del riesgo y el diseño de controles en entidades públicas. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Guía No.7 Seguridad y Privacidad Información-MINTIC-2016.

NTC-ISO 31000-2009. Gestión del Riesgo, principios y directrices.

CONPES 3854 Política Nacional de Seguridad Digital

4. TÉRMINOS Y DEFINICIONES

Las definiciones y términos que se presentan a continuación han sido tomadas de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública- DAFP.

Activo de información: En el contexto de seguridad digital son activos los elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información-TIo Tecnologías de la Operación-TO que utiliza la organización para su funcionamiento.

Actividades de control: Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

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

Análisis de Riesgo: Determinar el impacto y la probabilidad del riesgo, dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Apetito al riesgo: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el Centro Cibernético Policial-CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

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

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.

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

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la Entidad.

Fraude: Sinónimo de engaño, inexactitud consciente, contra una persona u institución para obtener algún provecho, mientras que la otra parte es la perjudicada. La palabra fraude es de origen latín “fraus”. *(https://www.significados.com/fraude).*

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.

ICC: Es la denominación de lo que el CCOCI ha definido como Infraestructuras Críticas Cibernéticas en el ámbito colombiano.

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de la información de ser exacta y completa.

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

Líder o responsable del proceso: Persona con la responsabilidad y autoridad para gestionar un riesgo.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

Plan Anticorrupción y de Atención al Ciudadano-PAAC: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Plan de contingencia: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

Plan de manejo del riesgo: Plan de acción propuesto por el grupo de trabajo interno, cuya evaluación de beneficio costo resulta positiva y es aprobado por la Alta Dirección.

Política de Administración de Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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

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 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 medidas de tratamiento del riesgo.

Tolerancia al riesgo (niveles de aceptación): 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.*

Valorar el riesgo: Permite establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial. (Riesgo Inherente).

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

5. MARCO ESTRATÉGICO DE LA ART

Con el fin de establecer el contexto estratégico para la identificación de los riesgos, se presenta el marco estratégico de la ART a partir de la Planeación Estratégica de la ART, el modelo de operación por procesos, misión; visión; objetivos estratégicos y el levantamiento de los activos de la información de la Agencia.

5.1 Direccionamiento Estratégico

El Decreto 2366 de 2015 crea la Agencia para la Renovación del Territorio – ART, como una agencia estatal de naturaleza especial, del sector descentralizado de la Rama Ejecutiva del Orden Nacional, con personería jurídica, patrimonio propio y autonomía administrativa, técnica y financiera, adscrita al Ministerio de Agricultura y Desarrollo Rural.

La ART, tienen como objeto "coordinar la intervención de entidades nacionales y territoriales en zonas rurales afectadas por el conflicto priorizadas por el Gobierno nacional, a través de la ejecución de planes y proyectos para la renovación territorial de estas zonas, que permitan su reactivación económica, social y su fortalecimiento institucional para que se integren de manera sostenible al desarrollo del país". (Artículo 2º del Decreto 2366 de 2015).

Mediante Decreto 2107 de 2019, se modifica la estructura de la Agencia de Renovación del Territorio y crea la Dirección de Sustitución de Cultivos de Uso ilícito en la Agencia.

El artículo 281 de la Ley 1955 de 2019 del Plan de Desarrollo cambió la adscripción de la Agencia para Renovación del Territorio del Sector Agricultura y Desarrollo Rural al Sector Presidencia de la República.

Mediante Decreto 1223 del 4 de septiembre de 2020, se modifica la estructura de la Agencia de Renovación del Territorio

La ART, establece su direccionamiento estratégico, a partir del Decreto 2366 de 2015 "Por el cual se crea la Agencia de Renovación del Territorio, ART, se determina su objeto" y el Plan de Desarrollo 2018-2022 "Pacto por Colombia, pacto por equidad".

5.2 Misión y Visión

Misión. Gerenciar procesos para la transformación de los territorios priorizados mediante la articulación entre la Nación y el territorio y el fortalecimiento de las capacidades de los actores en las subregiones PDET.

Visión. En el 2031, habremos logrado el mejoramiento de la calidad de vida de la población y el fortalecimiento de las capacidades de gobernanza de las subregiones PDET a través de la ejecución de los Planes de Acción para la Transformación Regional.

5.3 Objetivos estratégicos

Los objetivos estratégicos con los que se desarrolla la misión de la Agencia son los siguientes:

Implementar estrategias para la reactivación económica, social, ambiental e infraestructura rural en las zonas focalizadas por los programas de desarrollo con enfoque territorial - PDET nivel nacional.

Implementar estrategias de financiación y consolidación del Banco de proyectos para la implementación de los programas de desarrollo con enfoque territorial Nacional.

Implementar el esquema de seguimiento, evaluación y gestión de conocimiento para el cumplimiento de los PDET.

Coordinar y gestionar con los actores pertinentes a nivel nacional, territorial, públicas, privadas y de cooperación la implementación de las iniciativas resultantes de los PATR

Implementar estrategias de fortalecimiento de capacidades territoriales con los actores estratégicos y de acciones de incidencia en las instancias de planeación y participación territorial, para la estabilización en las zonas priorizadas por los municipios PDET.

Implementar un plan estratégico pedagógico, de divulgación y posicionamiento, que visibilice las transformaciones en los territorios, genere sentido de pertenencia y estimule la inversión en los PDET.

Garantizar una gestión efectiva que responda a las necesidades de los clientes con altos estándares de calidad.

Implementar el Programa Nacional Integral de Sustitución de Cultivos de Uso Ilícito-PNIS y nuevos modelos de sustitución en aquellos territorios que para el efecto determine el Consejo Directivo de la ART.

Líneas Estratégicas: La ART, estableció tres líneas estratégicas en las que se enfocarán las acciones para el cumplimiento de los objetivos institucionales estas son:

- Estructuración, ejecución y cofinanciación
- Articulación Nación-Territorio
- Apoyo Transversal
- Sustitución de Cultivos ilícitos

5.4 Modelo de operación por procesos – mapa de procesos de la ART

El Comité Directivo de la Agencia de Renovación del Territorio –ART, en reunión del 5 de octubre de 2017, aprobó el Modelo de Operación por procesos y el Mapa de Procesos de la ART, el cual quedó conformado por cuatro (4) Macro-procesos y quince (15) procesos así:

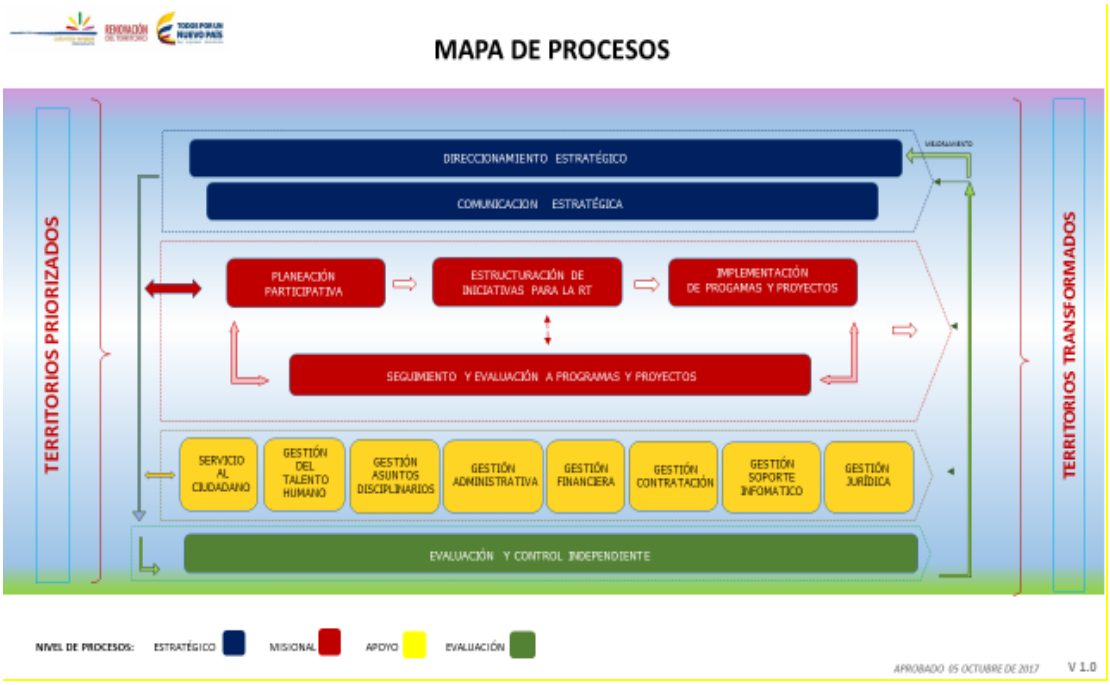
Dos (2) Estratégicos

Cuatro (4) Misionales

Ocho (8) de Apoyo

Uno (1) de Evaluación

Estos se pueden identificar en el Mapa de Proceso de la ART.



Fuente: Información Agencia de Renovación del Territorio.

La Gestión de Riesgos de la Agencia de Renovación del Territorio, basa su operatividad a partir del Modelo de Operación por procesos y el Mapa de Procesos que la Entidad haya aprobado, cuando se actualice o modifique la estructura de operación por procesos de la Agencia, los mapas de riesgos por procesos son actualizados de acuerdo con las modificaciones realizadas a los procesos.

6. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS – ART

La política de administración de riesgos de la ART es establecida por la Alta Dirección en cabeza del Representante Legal y en el marco del Comité Institucional de Coordinación de Control Interno de la Entidad.

"La Agencia de Renovación del Territorio, se compromete a adoptar y cumplir los lineamientos y directrices que se establecen a través del presente Manual, como instrumento para la adecuada administración de riesgos, mediante la implementación de actividades de prevención, sensibilización y control, que permitan el cumplimiento de los objetivos y misión institucional."

La política de administración de riesgos de la ART establece los niveles de responsabilidad para la gestión de riesgos, mediante el esquema de las líneas de defensa; la metodología para la identificación, valoración y niveles de tolerancia de los riesgos residuales; las acciones a seguir para mitigar la materialización de estos y establecer medidas frente a los posibles riesgos de gestión, corrupción y riesgos de seguridad digital.

Como parte de la Política, la Alta Dirección de la ART y su equipo de trabajo, se comprometen a:

✓ Liderar la gestión de riesgos en todos los procesos, programas, proyectos y Grupos Internos de Trabajo-GIT de la ART, en cumplimiento con las normas establecidas por el DAFP, acordes con la legislación vigente y la normatividad aplicable a la Entidad.

✓ Establecer e implementar las metodologías necesarias para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos de gestión, de corrupción y de seguridad digital, como instrumento para una adecuada gestión integral de riesgos.

✓ Establecer, mantener, socializar y difundir las estrategias de mitigación o tratamiento de los riesgos, que garanticen en forma razonable la eficacia de las acciones planteadas para evitar la posible materialización de los riesgos identificados.

✓ Promover los principios y valores éticos, establecidos en el código de integridad de la ART, en todos los niveles de la organización y establecer las acciones pertinentes, en pro de prevenir posibles actos de fraude y/o corrupción en la Entidad.

✓ Vigilar el cumplimiento y entendimiento de las normas y políticas, así como divulgar y socializar en toda la Entidad la misión, visión, políticas y procedimientos a todos los servidores públicos que presten sus servicios en la ART, con el fin de mitigar y minimizar los riesgos en cada uno de los procesos de la ART.

✓ Fomentar y mantener canales de comunicación efectivos, que permitan generar conciencia en todos los niveles de la ART sobre la importancia y relevancia de la efectiva gestión del riesgo en la Entidad.

✓ Analizar los resultados de las evaluaciones realizadas a la Entidad por los organismos de control, como fuente generadora para identificar posibles riesgos, que puedan afectar el cumplimiento de los objetivos y metas institucionales.

Importancia de la Gestión de Riesgos

✓ Permite identificar de manera oportuna los eventos potenciales tanto internos como externos que puedan afectar el cumplimiento de los objetivos y misión institucional.

✓ Evita que los eventos negativos, lesionen la imagen institucional, entorpezcan la operación, el cumplimiento de los objetivos estratégicos y metas institucionales o que afecten la prestación de los servicios.

✓ Permite, controlar y dar tratamiento prioritario a los riesgos de gestión y de seguridad digital de mayor incidencia y los relacionados con los riesgos de corrupción.

✓ Potencializa los eventos positivos, para que permitan minimizar el impacto de los posibles eventos negativos en la gestión de los riesgos.

✓ Identifica, disuade y detecta posibles fraudes que puedan afectar la adecuada gestión de la Entidad.

✓ Incrementa la confianza de todos los procesos de la ART en el uso del entorno digital.

✓ Genera mecanismos que permiten el aseguramiento de los activos de información de la Agencia.

6.1 TOLERANCIA DE LOS RIESGOSO NIVELES DE ACEPTACIÓN

De acuerdo con la calificación de los riesgos residuales (riesgos después de controles), la ART establece los niveles de aceptación para cada uno y el plan de manejo o tratamiento de los riesgos, aplicables para los riesgos de gestión, de corrupción los de seguridad digital.

6.1.1 Niveles de aceptación o tolerancia de los riesgos.

Para el adecuado tratamiento de los riesgos, la Agencia de Renovación del Territorio- ART, establece los niveles de aceptación y tolerancia para los riesgos para cada caso así:

Riesgos de Gestión y de Seguridad Digital

Riesgos de Corrupción. Para los riesgos de corrupción, sólo se tendrán dos clases de niveles de aceptación:

- **Evitar o reducir el riesgo.** Estos niveles de aceptación, independiente de la calificación de los riesgos residuales.
- Los riesgos de Corrupción no admiten aceptación, compartir o transferir el riesgo y siempre generan tratamiento.

6.1.2 Tratamiento o manejo de los riesgos.

A continuación, se presenta el manejo o tratamiento de los riesgos para la ART, de acuerdo con la calificación después de controles (riesgos residuales), los cuales se califican en zona de riesgo baja, zona de riesgo moderado, zonal de riesgo alta y zona de riesgo extrema. (La metodología para la valoración de los riesgos, se detalla en el **numeral 7.2 del presente manual**).

Para los riesgos de Seguridad Digital, de acuerdo con la zona que se califique el riesgo, se establece los niveles y el tratamiento que se debe dar, con el fin de evitar su materialización, reducir la zona del riesgo o eliminar el riesgo.

Se debe realizar en primera medida la identificación de los riesgos de seguridad digital para luego definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los niveles establecidos.

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos residuales priorizados, con el fin de optimizar los recursos disponibles y enfocar los esfuerzos institucionales, la ART establece como prioridad el tratamiento de los riesgos de seguridad digital ubicados en las zonas de riesgo altas y extremas.

Tratamiento riesgos de gestión y seguridad digital

Calificación del Riesgo	POLÍTICA (niveles de aceptación)	Plan de Manejo o tratamiento del Riesgo
ZONA BAJA	**ASUMIR O ACEPTAR EL RIESGO**	Riesgos inherentes, no se requiere adoptar medidas para su tratamiento. Realizar monitoreos periódicos (semestrales o trimestrales) al riesgo para que permanezcan en zona baja o se permita eliminar el riesgo.
ZONA MODERADA	**REDUCIR EL RIESGO**	Establecer acciones, medidas que permitan reducir la probabilidad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre a los riesgos y controles. Optimizar los procedimientos de seguridad digital establecidos.
ZONA ALTA	**EVITAR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los riesgos y controles. Realizar mantenimiento preventivo a la infraestructura tecnológica.

ZONA EXTREMA	**EVITAR EL RIESGO** **COMPARTIR O TRANSFERIR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando tanto la probabilidad y/o impacto. Monitoreo mensual a los controles y riesgos y establecer planes de contingencia en caso de materialización. Realizar Contratos de Mantenimiento correctivo, y de soporte sobre la plataforma tecnológica con proveedores. Establecer Contratos de seguro.

Fuente: Agencia de Renovación del Territorio- ART 2019

Tratamiento riesgos de corrupción

Calificación del Riesgo del Riesgo	POLÍTICA (niveles de aceptación) de aceptación)	Plan de Manejo o tratamiento del Riesgo
ZONA BAJA	REDUCIR EL RIESGO	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.
ZONA MODERADA		
ZONA ALTA	EVITAR EL RIESGO	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los riesgos y los controles. Establecer planes de contingencia para aplicar en caso de materialización.
ZONA EXTREMA	COMPARTIR O TRANSFERIR EL RIESGO	

Fuente: Agencia de Renovación del Territorio- ART 2019

6.1.3 Tratamiento a los riesgos materializados

En caso de materialización de los riesgos de gestión, de corrupción o de seguridad digital la ART, determina las siguientes acciones a seguir para su tratamiento.

Riesgos de Gestión	Riesgos de Corrupción y/o Fraude	Riesgos de Seguridad Digital
Establecer las acciones correctivas pertinentes. Poner en marcha los planes de contingencia, para los riesgos que cuenten con ellos. Revisar el Mapa de Riesgos del proceso y en particular, los riesgos, causas y solidez de los controles.	Informar a las instancias y autoridades pertinentes de la ocurrencia del hecho de corrupción. Establecer las acciones correctivas pertinentes. Revisar el Mapa de Riesgos de Corrupción, en particular, los riesgos, causas y solidez de los controles. Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción. Realizar un monitoreo permanente.	Informar al líder del proceso sobre el suceso. Informar a las instancias y autoridades pertinentes si es ataque informático. Poner en marcha los planes de contingencia, restauración y respaldo para los riesgos que cuenten con ellos. Revisar el Mapa de Riesgos del proceso en particular, los riesgos, causas y solidez de los controles. Establecer y documentar las acciones correctivas pertinentes.

Fuente: Adoptado de la Guía para la administración de riesgos y diseño de controles-DAFP 2018

6.1.4 Roles y responsabilidades

La ART, estructura los criterios para la adecuada toma de decisiones respecto al tratamiento de los riesgos y sus efectos al interior de la Entidad, por lo tanto, la implementación y mantenimiento de la Política de Administración de Riesgos, la metodología y tratamiento de los mismos, debe ser establecida por la Dirección con el apoyo del equipo directivo, el equipo operativo (líderes de proceso y gestores del Sistema de Gestión) y debe ser interiorizada por todos los servidores públicos y contratistas de la Entidad, responsables del desarrollo de actividades de los diferentes procesos.

Para la adecuada gestión de los riesgos de gestión, corrupción y de seguridad digital, la ART define los roles y responsabilidades para las líneas de defensa, con el fin implementar, coordinar, revisar, monitorear, hacer seguimiento y evaluar los riesgos inherentes a cada proceso.

LÍNEA ESTRATÉGICA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
ALTA DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO Representante Legal Equipo Directivo (que hace parte del Comité Institucional de Coordinación de Control Interno CICCI.)	Establecer y aprobar la Política de Administración de Riesgos de la ART, con la participación del Comité Institucional de Control Interno y el liderazgo del Representante Legal. Establecer los lineamientos y metodología para el tratamiento, manejo y seguimiento de los riesgos, incluyendo los riesgos de gestión, corrupción y de seguridad digital, que puedan afectar el logro de los objetivos institucionales. Establecer los roles y las responsabilidades frente a la Gestión de Riesgos de la Entidad incluyendo el responsable de Seguridad de la Información para la efectiva administración de los Riesgos de SD. Difundir y realimentar al CIGD sobre los resultados del seguimiento a los riesgos y la toma de decisiones, para los ajustes a los riesgos. Revisar y analizar los cambios en el "Direccionamiento estratégico", para la identificación de nuevos riesgos o la modificación de los que ya se tienen identificados, considerando los cambios en el entorno y los riesgos emergentes, que puedan afectar el cumplimiento de los objetivos estratégicos. Analizar los resultados del seguimiento de los riesgos estratégicos y de mayor impacto, para tomar acciones estratégicas que permitan mitigar la ocurrencia de los riesgos. Revisar en forma periódica la Política de Administración de Riesgos de la Entidad. Revisar en forma periódica el resultado del cumplimiento de los objetivos estratégicos y metas institucionales y de procesos, así como de los indicadores, para identificar posibles riesgos que se están materializando por no cumplimiento de estos.

PRIMERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
LÍDERES DE PROCESO GERENTES PÚBLICOS, GERENTES DE PROYECTOS O PROGRAMAS	Asegurar que la Política para la gestión de riesgos, se socialice a los integrantes de sus equipos de trabajo y se implemente adecuadamente dentro del proceso. Analizar y establecer los objetivos de los procesos, para que estén alineados con la Misión y la Visión y asegurar que contribuyan a los objetivos estratégicos. A partir del contexto estratégico, analizar e identificación los riesgos que puedan afectar el cumplimiento del objetivo de su proceso, teniendo en cuenta los riesgos de gestión, corrupción y de seguridad digital. Comunicar a la segunda línea de defensa los eventos o desviaciones en la gestión de los riesgos y en especial en caso de materialización de riesgos de fraude y corrupción, para la toma de acciones pertinentes. Desarrollar e implementar procesos de control y gestión de riesgos a través del análisis, valoración, tratamiento, monitoreo y acciones de mejora, para la mitigación de los riesgos del proceso Identificar los activos de información de cada proceso, para la gestión adecuada de los riesgos de seguridad digital, conforme a la metodología establecida por la Línea Estratégica. Verificar y monitorear los controles de los riesgos del proceso(gestión, seguridad digital y de corrupción), y determinar que se estén ejecutando tal como han sido diseñados. Verificar el desarrollo y mantenimiento de controles de los riesgos de Seguridad Digital, ésta actividad corresponde al Oficial de Seguridad de la Información o quien haga sus veces en la Entidad. Monitorea que los Planes de manejo de los riesgos se ejecuten adecuadamente por los responsables y determina su efectividad.

SEGUNDA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
OFICINA DE PLANEACIÓN	Asesorar a la línea estratégica en el análisis del contexto interno y externo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo Apoyar a la Alta Dirección en la estructuración y definición de la Política de Administración de riesgos de la ART, para presentarla al Comité Institucional de Control Interno- CICCI Consolidar el Mapa de riesgos Institucional con los riesgos de mayor criticidad de gestión y de seguridad digital y los riesgos de corrupción y fraude. Realizar la difusión y asesoría de la metodología para la gestión de riesgos adoptada por la ART, así como de orientar a los líderes de proceso en el establecimiento de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad y asegurar su implementación. Fomentar la administración del riesgo como una actividad inherente al proceso de Planeación Estratégica, trabajando en forma coordinada y armónica con la Oficina de Comunicaciones y el Grupo de Control Interno. Orientar y acompañar a los líderes de procesos en la gestión de riegos (gestión, corrupción y de seguridad digital) en cada una de sus etapas (Identificación, análisis, evaluación, establecimiento de controles y planes de manejo). Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan que la implementación de los planes de manejo de los riesgos sean eficaces. Revisa los cambios en el direccionamiento estratégico o en el entorno y determina si pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos y apoyar la actualización de las matrices de riesgos.
COORDINADORES DE GIT. Supervisores de Contratos,	Conocer y apropiar la política institucional de gestión de riesgos. Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente revisar el adecuado diseño de los controles. Asegurarse de que la Política y metodología para la Gestión de riesgos adoptada por la Entidad, se difunda e implemente adecuadamente en los dentro de sus equipos de trabajo. Participar en las actividades de socialización y programas de aprendizaje que se programen, relacionados con riesgos. Asegurar la implementación efectiva de los controles y las acciones preventivas necesarias para evitar la materializaciones de riesgos (Autogestión). Hacer seguimiento a las actividades de manejo para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. Informar sobre las alertas que se presenten en la ejecución de los planes de manejo propuestos y en la ejecución de controles. Supervisores: alertar sobre la posible materialización de los riesgos identificados en la ejecución de los contratos

TERCERA LÍNEA DE DEFENSA	
ROLES	**RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS**
GRUPO INTERNO DE TRABAJO DE CONTROL INTERNO	Trabajar en coordinación con la Oficina de Planeación y Líderes de proceso en la difusión y socialización de la Política y metodología de Administración de Riesgos de la Entidad Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. Comunicar a la Alta Dirección, sobre el resultado de la evaluación a la gestión de riesgos y los posibles cambios e impactos, en el cumplimiento de los objetivos institucionales. (riesgos de corrupción y posibles fraudes) Proporcionar 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. Le corresponde al GIT de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la Entidad, a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Evaluar la eficacia de la gestión de riesgos en la Entidad, el diseño y efectividad de los controles e informar a la Dirección sobre la efectividad de los mismos. Realizar el seguimiento a los riesgos de gestión, seguridad digital de acuerdo con la periodicidad que se determine y priorizando los riesgos con mayores niveles de riesgo y a los riesgos de corrupción, según las fechas establecidas en la Metodología para la construcción del PAAC.

Además de las líneas de defensa y las responsabilidades asignadas para la Administración de Riesgos, a continuación, se presentan las responsabilidades establecidas en el Modelo de Seguridad y Privacidad de la Información MSPI- dadas en la Estrategia de Gobierno Digital del MINTIC, al responsable de Seguridad Digital, quien debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica. [1]

El responsable de Seguridad Digital será quien tenga las siguientes responsabilidades respecto a la Gestión de Riesgos de Seguridad Digita-GRSDI:

RESPONSABILIDADES RIESGOS DE SEGURIDAD DIGITAL		
ROLES Y RESPONSABILIDADES DE SEGURIDA DIGITAL		
PRIMERA LÍNEA DE DEFENSA	**RESPONSABLE DE LA SEGURIDAD DIGITAL**	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.
SEGUNDA LÍNEA DE DEFENSA	**OFICIAL DE SEGURIDAD**	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento). Definir el procedimiento o metodología para la Identificación y Valoración de Activos. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información

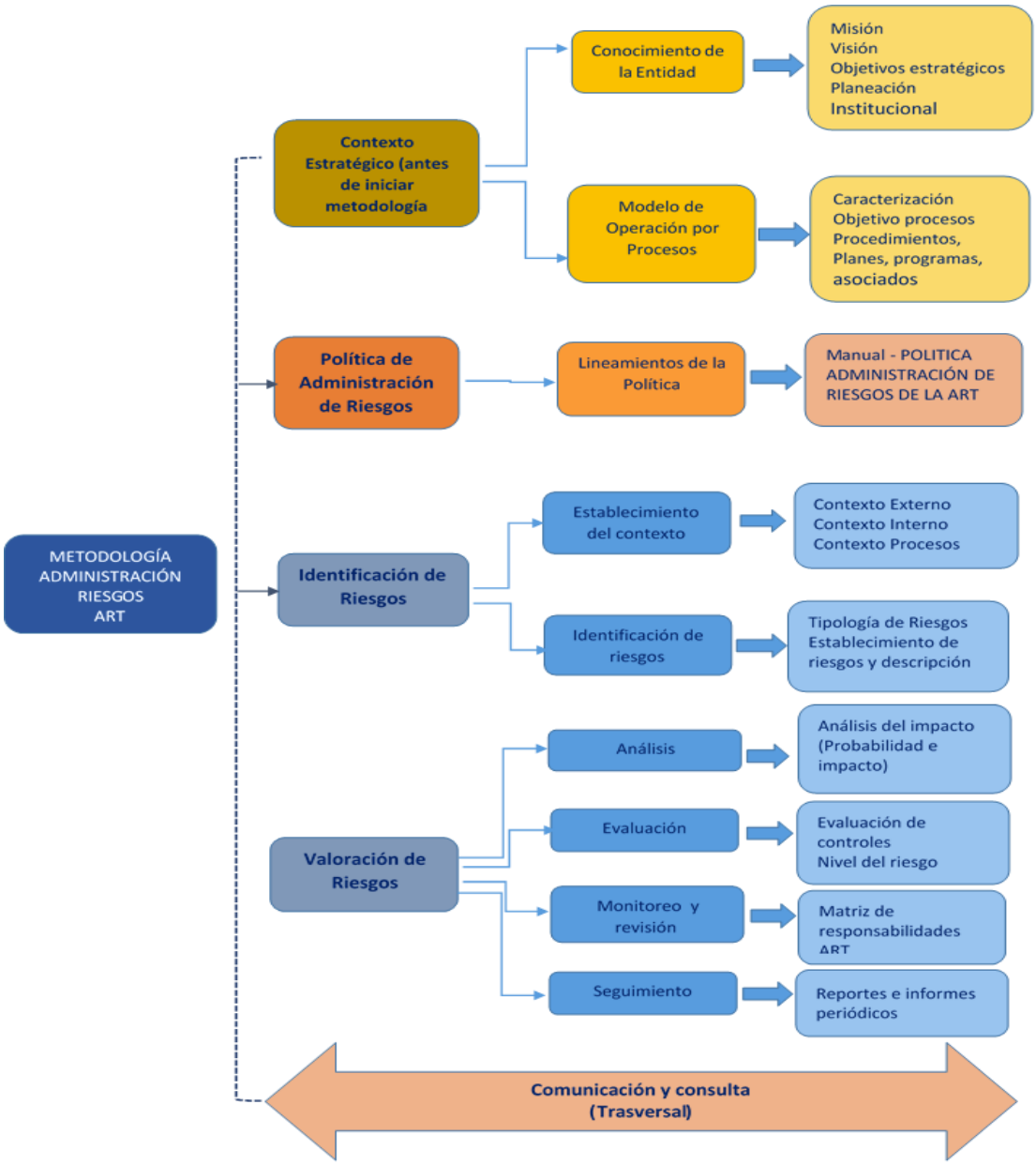
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

[1] **Anexo 4. Lineamientos para a Gestión de Riesgos de SD en Entidades Públicas-MINTIC-2018**

7. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS– ART

La Agencia para la Renovación del Territorio, para la adecuada administración de riesgos adopta la metodología establecida por el DAFP, en la Guía para la Administración del Riesgo y Diseño de controles en entidades públicas-2018 del DAFP y la Estrategia para la Construcción del Plan Anticorrupción y Atención al Ciudadano V.2- 2015, el cual complementa la metodología respecto de los riesgos de corrupción.

Esquema para la Gestión de riegos



Fuente: ART-2019 Adaptado de la Guía para la administración de riesgos y diseño de controles-DAFP 2018

Esquema para la Gestión de riesgos Digitales

La Oficina de Planeación, establecerá la herramienta o la matriz para el manejo de los riesgos, la cual contendrá los componentes relacionados con la identificación, valoración y el plan de manejo para los riesgos.

De acuerdo con lo anterior, se estructuró la matriz para la identificación, valoración y planes de manejo con sus respectivos campos FM-DE-08, así mismo, resultado de ésta, se genera el formato de Mapa de Riesgo de proceso FM-DE-09 y contiene los respectivos anexos para la gestión de riesgos los cuales hacen referencia a:

Anexo No.1 Criterios para calificar el impacto de los riesgos de corrupción

AnexoNo.2 Evaluación de Controles

Anexo No.3 Análisis solidez de controles

Anexo 4 Calificación de riesgos

Anexo 5 Tratamiento de riesgos

Anexo 6 Definiciones

Para los respectivos mapas de riesgo de proceso (FM-DE-08), de corrupción (Formato FM-DE-14).

Para la gestión de los riesgos de Seguridad Digital-RSD, se estructuró la matriz para la identificación, valoración y planes de manejo con sus respectivos campos FM-DE-22, así mismo, resultado de ésta, se genera el formato de Mapa de Riesgo de proceso de SD.FM-DE-22 y contiene los respectivos anexos para la gestión de riesgos los cuales hacen referencia a:

AnexoNo.1 Evaluación de Controles

Anexo No.2 Análisis solidez de controles

Anexo No.3 Calificación de riesgos

Anexo No.4 Tratamiento de riesgos

Anexo No.5 Definiciones

Clases de Mapas

El mapa de riesgo por procesos FM-DE-08, estará bajo la responsabilidad de cada uno de los líderes, el cual será consolidado por la Oficina de Planeación y estará conformado por los riesgos de gestión y los riesgos de corrupción de cada proceso.

El mapa de riesgos de Corrupción FM-DE-014, es consolidado por la Oficina de Planeación y está conformado por los riesgos de corrupción identificados en los diferentes procesos de la Entidad.

El mapa de riesgos de Seguridad Digital-RSD, FM-DE-22, estará bajo la responsabilidad de cada uno de los líderes, con el apoyo y orientación del responsable de seguridad digital y será consolidado por la Oficina de Planeación. Estará conformado por los riesgos de SD, calificados en zona Alta y Extrema.

El mapa de riesgos Institucional es consolidado por la Oficina de Planeación y está conformado por los riesgos residuales, que se encuentren en una zona de riesgo, moderada, alta o extrema de los riesgos de gestión; en zona Alta o Extrema de los riesgos de SD y los riesgos de corrupción.

El mapa de riesgo Institucional recopila los planes de manejo de los riesgos de cada proceso y los cuales son susceptibles de seguimiento por parte de la Oficina de Planeación y el GIT de Control Interno y presenta el resultado del monitoreo y seguimiento periódicos que se realice a los riesgos de proceso.

La Oficina de Planeación, publicará los mapas de riesgos de proceso, de Seguridad Digital, e institucional, en el repositorio MERCURIO/SIGART en el link del MIPG y el mapa de riesgos de corrupción se publicará en la página web de la Entidad, en el link de transparencia, de acuerdo con lo establecido en la Ley 1712 de 2014 y el Decreto 103 de 2015 y la Ley 1474 de 2011.

7.1 Identificación y análisis de riesgos

La identificación de los riesgos tiene como objetivo, identificar las fuentes, eventos de riesgos, sus causas y consecuencias, que puedan incidir en la consecución de los objetivos de los procesos.

Esta etapa, inicia con el establecimiento del contexto estratégico de la entidad y de proceso, una vez se establece, se inicia con la construcción de los riesgos por procesos, sus causas y consecuencias.

7.1.1. Tipología de Riesgos

La tipología de riesgos asociados a los procesos, de la Entidad es[2]:

Riesgos de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.

Riesgos Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impacta toda la entidad,

Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos.

Riesgos Financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Imagen o reputacional: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante los clientes y partes interesadas.

Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

[2] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2018**

Las pérdidas asociadas a este tipo de riesgo pueden originarse en fallas de los procesos, en la tecnología, en la actuación de la gente, y también, debido a la ocurrencia de eventos[3].

Riesgos de Cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos Tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgos de seguridad digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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.

7.1.2. Establecimiento del contexto estratégico.

La identificación del riesgo debe ser un proceso permanente, para establecer el contexto estratégico de la ART, se parte del conocimiento estratégico de la Entidad, la misión, la visión y los objetivos estratégicos, a partir de los cuales se identifican los factores o eventos internos o externos, que pueden ocasionar riesgos que afecten el logro de los objetivos institucionales.

Para la identificación de los riesgos de proceso, se pueden involucrar datos históricos, análisis teóricos, opiniones informales y expertas, planeación institucional, mapa de procesos, caracterizaciones, procedimientos, entre otros, a fin de conocer con claridad el entorno, para establecer los eventos que pueden tener incidencia en el cumplimiento de los objetivos del proceso y proyectos.

Contexto externo: Este inicia con el análisis y establecimiento de los factores externos que puedan afectar a la Entidad para el cumplimiento de la misión y objetivos institucionales.

[3] https://es.wikipedia.org/wiki/Riesgo_operativo

Los factores externos pueden ser:

CLÁSIFICACIÓN	FACTORES
EXTERNOS	**Económicos y financieros:** asignación presupuestal, liquidez, austeridad en el gasto.
	Políticos: Decisiones gubernamentales, no continuidad en los programas de gobierno, cambios en el gobierno.
	Socioculturales: Ubicación de las zonas priorizadas, acciones o actividades culturales en los territorios, idiomas, etnias, entre otros.
	Legales: Cambios normativos y legales aplicables a la Entidad, legislación, regulación.
	Tecnológicos: Planes estratégicos de Tecnologías de la información, Falta de comunicación con los territorios, No implementar la estrategia de Gobierno Digital, sin recursos para la Transformación Digital.
	Medioambientales: Ambiente y estados del clima en los territorios que afecten el desarrollo de las actividades. (Catástrofes naturales-Lluvias, inundaciones, verano, entre otros). Sostenibilidad ambiental.
	Comunicación externa. Insuficientes o dificultades en canales de comunicación con los territorios y zonas priorizadas.
	Orden público: Acciones de terceros (grupos al margen de la ley, paros de la población, entre otros) que dificulten el desarrollo de las actividades
	Fuerza mayor o caso fortuito: Factores externo no controlados e imprevisibles que pueden afectar el cumplimiento de los objetivos. (acciones de la naturaleza, salud pública, etc.)
	Entorno digital: Afectaciones por fallas sistemas de información, sitio web, plataformas, etc.

Contexto interno: Se tiene en cuenta las condiciones internas que puedan afectar el cumplimiento de la misión, objetivos estratégicos, procesos de la Entidad (Estratégicos, Misionales, Apoyo y Evaluación), cumplimiento de procedimientos.

De los factores internos se identifican:

CLÁSIFICACIÓN	FACTORES
INTERNOS	**Estructura organizacional:** Diseño, niveles organizacionales que respondan al objeto, funciones, organización de la entidad.
	Funciones y responsabilidades: Desagregación adecuada de funciones y responsabilidades.
	Financieros: Ejecución presupuestal, demora asignación de recursos y apropiaciones, etc.
	Personal: Temas de capacitación, clima organizacional, planta de personal, rotación, funciones y responsabilidades, entre otros.
	Tecnología: Deficiencias en la infraestructura tecnológica, recursos para los servicios tecnológicos insuficientes o no óptimos, No Implementación del Modelo de seguridad y privacidad de la información, Sin lineamientos de Gobierno TI.
	Estratégicos. Fallas en la Planeación, metas no adecuadas, mapa desactualizado, estructura organizacional no acordes con los procesos, indicadores mal formulados no permiten el seguimiento y toma de decisiones, no existen de políticas o no son observadas, etc.
	Operación de procesos: Interacción de procesos, procedimientos asociados, desactualización de documentos, etc.
	Comunicación interna: Falencias en los canales de información interna, demoras o fallas en la comunicación de la información hacia los diferentes niveles y sectores de la organización, etc.
	Niveles de autoridad. Grado de responsabilidad frente a los procesos, delimitación de los niveles de autoridad

Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

CLÁSIFICACIÓN	FACTORES
CONTEXTO DEL PROCESO	**Diseño del proceso:** Claridad en la descripción y objetivo del proceso.
	Interacción con otros procesos: relación precisa con otros procesos, insumos, proveedores, productos, etc.
	Transversalidad: De procesos que definen lineamientos para el desarrollo de todos los procesos de la Entidad. **(**estratégicos, de evaluación)
	Procedimientos asociados: Pertinencia de los procedimientos para el desarrollo de los procesos.
	Responsabilidad de procesos: definición adecuada de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre procesos: efectividad en los flujos de información determinados en la interacción de los procesos.
	Activos de seguridad de la información: información, aplicaciones, software, hardware, servicios, redes, bases de datos, información física y digital, entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso y de cara al ciudadano.

Para la identificación de los riesgos estratégicos que pueden afectar el cumplimiento de los objetivos estratégicos de la entidad, se inicia con la identificación de los mismos, a partir de los objetivos estratégicos que apunta a cada proceso y el análisis del contexto estratégico.

Los riesgos estratégicos, se identifican y hacen parte del mapa de riesgos de cada proceso, permitiendo la adecuada gestión y monitoreo por parte de los líderes, así mismo, a través de los planes

de manejo, mitigar su materialización, lo cual genera confianza en el desarrollo de las actividades organizacionales para cumplimiento de los objetivos estratégicos.

7.1.2 Análisis de riesgos de gestión.

La construcción de los riesgos se realiza a partir de la identificación del contexto estratégico, tomando como base los procesos establecidos en la Entidad, el conocimiento de situaciones del entorno y contexto interno de los procesos, una vez se tiene, se determinan las causas generadoras de los riesgos que pueden afectar el logro de los objetivos de los procesos y procedimientos asociados y las consecuencias en caso de materialización.

A partir de la definición de los factores internos y externos, se puedan enlistar los eventos asociados al objetivo del proceso, sus causas y consecuencias.

Para llevar a cabo la identificación, se recomienda dar respuesta a los siguientes interrogantes:

- **¿Qué puede suceder?** Eventos que pueden afectar el cumplimiento del objetivo del proceso o de la misionalidad.
- ¿**Cómo puede suceder?** Identificar las causas que puede ocasionar los riesgos, a partir de los factores del contexto.
- **¿Cuándo puede ocurrir?** En qué momento puede suceder en el desarrollo del proceso o procedimiento asociado.
- **¿Qué consecuencias traería su ocurrencia?** Se definen los posibles efectos o consecuencias en caso de materialización del riesgo.

Para identificar los riesgos, la redacción de los mismos debe evitar las palabras negativas como:

“No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente” [4].

Para el análisis de las causas que originan la materialización de los riesgos, primero se identifican las actividades más relevantes, críticas o factores de éxito que pueden contribuyen o impactan el cumplimiento de los objetivos de los procesos.

Una vez se identifican estas actividades, se continúa con la priorización de causas más probables que pueden incidir en la materialización de los riesgos identificados, se puede utilizar los métodos o herramientas de:

- Tres (3) o cinco (5) por qué
- Tormenta de ideas
- Lista de priorización

[4] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

7.1.3 Análisis de riesgos de corrupción

Para el establecimiento de los riesgos de corrupción, la ART toma como base, la metodología establecida en la Guía para la Administración de Riesgos y establecimientos de controles del DAFP, en relación con los riesgos de corrupción.

El riesgo de corrupción es "la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado"[5].

En la descripción de los riegos de corrupción concurran cuatro (4) componentes para su definición:

> ***Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.***

Para facilitar la identificación de los riesgos de corrupción, se cuenta con el Formato FM-DE-07 – ANALISIS DE RIESGOS DE CORRUPCIÓN en la cual se toman los riesgos identificados por cada proceso y se determina si el riesgo cumple con los cuatro componentes, en cuyo caso se trata de un riesgo de corrupción, de lo contrario, se trataría de un riesgo de gestión.

	ANÁLISIS RIESGOS DE CORRUPCIÓN						Código: FM-DE-07
	DIRECCIONAMIENTO ESTRATÉGICO						Versión: 03
	OFICINA DE PLANEACIÓN						Fecha de Publicación:
MACROPROCESO	PROCESO	Descripción del riesgo	COMPONENTES				OBSERVACIONES/ ACLARACIONES
			Acción u Omisión	Uso del Poder	Desviar la gestión de lo público	Beneficio particular	
ESTRATÉGICO							
MISIONAL							
APOYO							
EVALUACIÓN							

Fuente: Agencia de Renovación del Territorio- ART (adaptado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4.)

Una vez se haya realizado el ejercicio de la identificación de riesgos (gestión y corrupción), en el formato **FM-DE-08 V.5 Gestión de riesgos ART y Anexos**, se registran los riesgos identificados, para cada proceso, se clasifican de acuerdo con tipo de riesgo que pertenezca; las causas tanto internas como externas que generan los riesgos y las consecuencias en caso de materialización.

[5] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

IDENTIFICACIÓN Y ANÁLISIS					
No.	RIESGO	CLASE DE RIESGO	CAUSAS		CONSECUENCIAS
			EXTERNAS	INTERNAS	

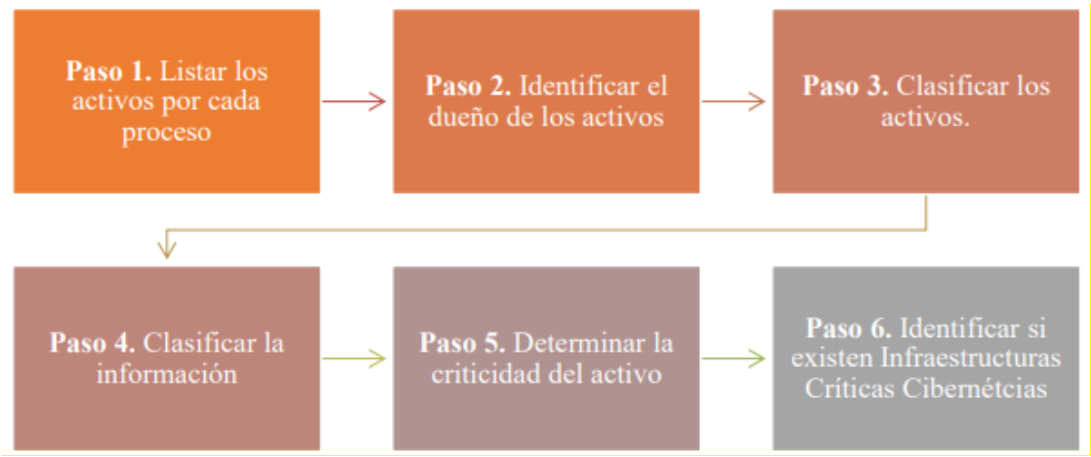
Fuente. Formatos ART- FM-DE-08 V.5 –ART 2020

7.1.4 Análisis de riesgos de Seguridad Digital

El análisis de riesgos de seguridad digital para la ART se realiza en base al Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MGRSD, establecido por MINTIC y ANEXO 4: Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas de Función Pública.

7.1.4.1. Identificación de los activos.

En la aplicación de este modelo se establece la identificación de los Activos de Información de la Agencia teniendo en cuenta los siguientes pasos para su identificación:



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Nota: Cada uno de estos pasos se encuentran descritos en la guía técnica de los activos de información de la Agencia que se encuentra en la carpeta SIGART del servidor Mercurio.

Identificación de Infraestructuras Críticas Cibernéticas (ICC).

Una vez realizada la identificación, clasificación y valoración de los activos de información, y determinada la importancia de estos para la Agencia, el proceso encargado del inventario de activos

identifica si cuenta con ICC o si alguno de los activos identificados corresponde a una ICC y verifica si su impacto o afectación supera alguno de los criterios siguientes:

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: Identificación de Infraestructuras Críticas Cibernéticas (ICC). Fuente: Modelo de Gestión de Riesgos de Seguridad Digital-MINTIC

Impacto Social: La variable de población se define teniendo en cuenta el establecimiento del contexto externo de la ART, es decir, que la consideración de la población va a estar asociada a las personas a las cuales se les presta servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectados por la materialización de algún riesgo en los activos identificados como ICC.

Impacto Económico: La variable presupuesto es la consideración del presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

Impacto Ambiental: La variable ambiental estará alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Podría no ser utilizada en la mayoría de los casos.

Nota. Si la entidad cuenta con ICC esta es reportada al CCOCI

ID ACTIVO	NOMBRE DEL ACTIVO	NIVEL DE CRITICIDAD/ ACTIVO	ICC			
			SOCIAL 250.000 personas	ECONÓMICO	AMBIENTAL	SE DEBE REPORTAR CCOCI
Indicar ID del Activo	Indicar Nombre del Activo	Indicar Nivel de criticidad, definido en tabla de registro de activos	Indicar con **x** si hay afectación social	Indicar con **x** si hay afectación económica	Indicar con **x** si hay afectación ambiental	Indicar con **x** si se debe reportar a CCOCI

7.1.4.2 Metodología para la identificación de riesgos de SD.

El propósito de la identificación de los riesgos de Seguridad Digital-RSD, es determinar que podría suceder para que cause una perdida potencial, y llegar a comprender el cómo, el dónde, y el por qué podría ocurrir está perdida. Las siguientes etapas del análisis de riesgos de SD se requieren para recolectar datos de entrada para esta actividad.

Para la identificación de los riesgos inherentes, la ART tiene en cuenta las amenazas y vulnerabilidades asociadas a cada activo de información.

Se identifican tres (3) clases de riesgos inherentes a seguridad digital:

- **Integridad**: se refiere a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros no autorizados.
- **Confidencialidad**: se refiere a cómo los datos se mantienen al acceso únicamente de las personas o sistemas que se encuentran autorizados.
- **Disponibilidad**: se refiere al acceso de la información en el momento que debe estar disponible; se aclara que la información de la entidad no debe estar disponible todo el tiempo durante el año.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente se analizan las posibles amenazas y vulnerabilidades que podrían causar su materialización.

A continuación, se detallan algunas amenazas que pueden hacer daños a los activos y materializar los riesgos y algunas vulnerabilidades (debilidades) descritas en el *anexo 4. Lineamientos para la GRSD y complementadas por la Guía De Gestión De Riesgos emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Digital para la Seguridad y privacidad de la información:*

7.1.4.3. Identificación de las 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), fortuitas (F) o ambientales (A)
- ✓ Amenazas de tipo común
- ✓ Amenazas dirigidas por el hombre

Amenazas de tipo común:

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

Fuente: ISO/IEC 27005:2009

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

Fuente: ISO/IEC 27005:2009

7.1.4.4. Identificación de las Vulnerabilidades.

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)

Fuente: ISO/IEC 27005

De acuerdo con lo descrito en la *Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP,* para la identificación del riesgo y el análisis de las posibles amenazas y vulnerabilidades que podrían causar la materialización de este, la ART ha adoptado la siguiente tabla:

Riesgo	Descripción del riesgo	Activo	Tipo de Activo	Amenaza	Vulnerabilidades	Consecuencia/ Impacto
Identificar el tipo de riesgo de acuerdo con la identificación establecida	Detallar el riesgo	Asociar activo o grupo de activos según lo identificado en el formato de registro de activos de información	Detallar el tipo de activo de información	Detallar la amenaza a la cual está expuesta el grupo de activo	Describir cuales son las vulnerabilidades asociadas a la amenaza identificada.	Describir las consecuencias que tendría el grupo de activos al verse afectado por la amenaza asociada.

Una vez se haya realizado el ejercicio de la identificación de activos, se continúa con la identificación de los RSD, en el formato FM-DE-22 Matriz Riesgos de SD y Anexos , en la cual se registran los riesgos de SD y la información que se establece en la Matriz, para tal fin.

IDENTIFICACIÓN Y ANÁLISIS										
No.	RIESGO	DESCRIPCIÓN DEL RIESGO	NOMBRE DEL ACTIVO	PROPIEDAD DEL ACTIVO			TIPO DE ACTIVO	AMENAZAS (situación)	VULNERABILIDADES (Causas)	CONSECUENCIAS
				PROCESO PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	UBICACIÓN DEL ACTIVO				
1										
2										

Fuente. FM-DE-22 V.1 –ART 2020

7.2 Valoración de Riesgos

7.2.1. Análisis preliminar - Riesgo Inherente

La valoración de los riesgos inherentes consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, *antes de controles*, con el fin de estimar la zona de riesgo inicial.

La probabilidad es la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad [6]**.**

A continuación, se presenta el **ANEXO 4. TABLA VALORACIÓN DE RIESGOS** del formato FM-DE-08 y 09, la cual define la probabilidad según la frecuencia y el impacto en caso de materialización, para el análisis de los riesgos identificados.

[6] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

Definidas estas dos variables, se puede evaluar el riesgo.

ANEXO 4. TABLA VALORACIÓN DE RIESGOS				
PROBABILIDAD		**FRECUENCIA**	**IMPACTO**	
1	**Rara vez:** Puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos cinco(5) años.	**1**	**Insignificante:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	**Improbable:** Pudo y/o puede ocurrir en algún momento.	Al menos una vez en los últimos cinco (5) años.	**2**	**Menor:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	**Posible:** Podría ocurrir en algún momento.	Al menos una vez en los últimos dos (2) años.	**3 ***	**Moderado:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	**Probable:** Probablemente ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año.	**4 ***	**Mayor:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	**Casi seguro**: Se espera que ocurra en la mayoría de las circunstancias.	Más de una vez al año	**5 ***	**Catastrófico:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.
*	Los riesgos de corrupción, sólo tienen éstos tres nivels de impacto.			

Fuente: Agencia de Renovación del Territorio -2020

En la valoración de los riesgos de corrupción, el impacto sólo se tiene en cuenta los niveles Moderado, Mayor y Catastrófico, es decir 3, 4 y 5 respectivamente.

7.2.1.1. Criterios para análisis de impacto Riesgos de Corrupción.

A continuación, se presenta el **Anexo 1 CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN,** para establecer la zona de impacto de los riesgos de corrupción de acuerdo con las siguientes preguntas[7]**:**

[7] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

ANEXO 1. CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN		
PREGUNTA: SI EL RIESGO SE MATERIALIZA PODRÍA:	**SI**	**NO**
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, servicios o 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?		
17 ¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		
SUMA DE X's	0	0

Fuente: Adoptado Guía para la administración de riesgos y diseño de controles DAFP-2018 V4

Tabla de respuestas

CALIFICACIÓN IMPACTO	
RESPUESTAS POSITIVAS	**IMPACTO**
1 A 5	**MODERADO**
6 A 11	**MAYOR**
12 A 19	**CATASTRÓFICO**
Si la pregunta 16 es afirmativa es Catastrófico	

7.2.2. Calificación de los riesgos en la tabla de calor.

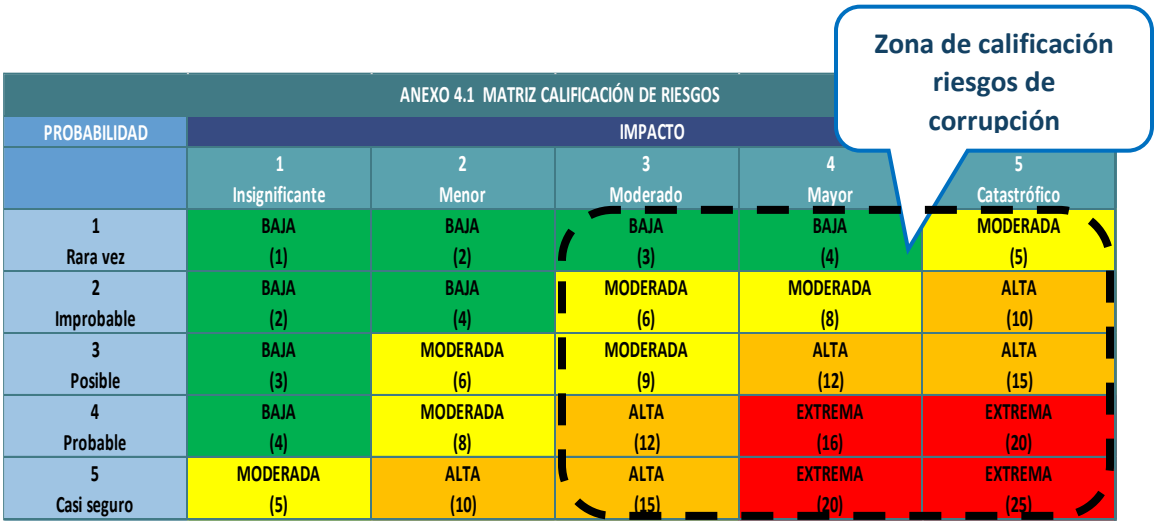
Para establecer la zona de calificación inicial de los riesgos inherentes, se cruzan los valores determinados para la probabilidad y el impacto de acuerdo con la tabla de valoración:

VALORACIÓN = Probabilidad X Impacto

Como resultado de la valoración de los riesgos inherentes, se pueden ubicar en zona:

BAJA	
MODERADA	
ALTA	
EXTREMA	

En el Anexo 4.1. Matriz calificación de riesgos del Formato FM-DE-08- al 09 Gestión de Riesgos y en el Formato **FM-DE-22 Gestión de Riesgos de Seguridad Digital**, se detallan las zonas de calificación de acuerdo con la probabilidad impacto de los riesgos inherentes.



ANEXO 4.1 MATRIZ CALIFICACIÓN DE RIESGOS					
PROBABILIDAD	IMPACTO				
	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
1 Rara vez	BAJA (1)	BAJA (2)	BAJA (3)	BAJA (4)	MODERADA (5)
2 Improbable	BAJA (2)	BAJA (4)	MODERADA (6)	MODERADA (8)	ALTA (10)
3 Posible	BAJA (3)	MODERADA (6)	MODERADA (9)	ALTA (12)	ALTA (15)
4 Probable	BAJA (4)	MODERADA (8)	ALTA (12)	EXTREMA (16)	EXTREMA (20)
5 Casi seguro	MODERADA (5)	ALTA (10)	ALTA (15)	EXTREMA (20)	EXTREMA (25)

Fuente: Agencia de Renovación del Territorio- ART 2019

Los riesgos de corrupción solamente se ubican en la matriz de calificación de riesgos en **MODERADA, MAYOR O CATASTRÓFICO.**

Una vez se obtiene la calificación y zona donde queda ubicado el riesgo inherente, se continúa con el establecimiento de controles y la valoración de los mismos, para determinar el riesgo residual (después de controles).

7.2.3 Establecimiento de controles.

Para minimizar la frecuencia o el impacto de los riesgos, se deben establecer los controles o actividades de control, los cuales permiten disminuir la frecuencia o minimizar el impacto de los riesgos.

Para el establecimiento de los controles se debe tener en cuenta:

- ✓ Para cada causa debe existir un control.
- ✓ Se deben trabajar en forma separada (no se deben combinar en una misma columna o renglón).
- ✓ Un control puede ayudar a mitigar varias causas, en estos casos el control se asocia a la causa de manera independiente.

Los controles se clasifican en:

Controles Preventivos: Son los que actúan para eliminar las causas del riesgo y prevenir su ocurrencia o materialización, como por ejemplo, el requerimiento de un login y password en un sistema de información; listas de chequeo.

Controles detectivos: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Estos permiten el restablecimiento de la actividad después de ser detectado un evento no deseable. Como ejemplo, las conciliaciones bancarias.

Las actividades de control tienen como fin:

- ✓ **Disminuir la probabilidad**: acciones encaminadas a gestionar las *causas* del riesgo.
- ✓ **Disminuir el impacto**: acciones encaminadas a disminuir las *consecuencias* del riesgo.

7.2.3.1 Establecimiento de controles de riesgos de Seguridad Digital

Para establecer los controles para los riesgos de Seguridad Digital se debe tener en cuenta:

- ✓ La selección de los controles implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar aspectos como:
- ✓ Viabilidad jurídica: Velar por que los controles que se van a implantar no vayan en contra de la normatividad vigente.

- ✓ Viabilidad técnica e institucional: Establecer claramente si la Agencia está en capacidad de implantar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.
- ✓ Análisis de costo-beneficio: Prácticamente todas las respuestas a los riesgos implican algún tipo de costo directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el costo inicial del diseño e implementación de una respuesta (procesos, personal, tecnología), así como el costo de mantener la respuesta de forma continua.
- ✓ Este caso se puede dar específicamente para aquellos controles nuevos que requieren contrataciones adicionales a los funcionarios que desarrollan los proceso o bien cuando se requiere diseñar e implementar sistemas de información o tecnologías específicas para ejecutar el control.

El Modelo de Seguridad y Privacidad de la Información de la ART en su fase de Planificación deberá realizar la selección de controles de seguridad digital que correspondan para el tratamiento del riesgo, y durante la fase Implementación deberá ejecutar la implementación de dichos controles, por lo cual se cuenta con el anexo de controles del estándar ISO 27001.

NOTA: *La Agencia deberá determinar si ya posee alguno de estos controles del Anexo A de la Norma ISO 27001 o si deberá aplicar alguno para realizar luego el tratamiento del riesgo residual.* ***El Anexo 1 Controles SD.,*** *del presente Manual se determina los controles que se ajustan a los existentes.*

A partir de esta metodología se establece una matriz de riesgos de seguridad digital que contempla la asignación de valores y atributos a la probabilidad de ocurrencia de una amenaza afectando la seguridad de los activos de información, al igual que los valores y atributos sobre el impacto que afectan a la Agencia, producto de la materialización de los riesgos. Adicionalmente, en la matriz se encuentran identificados los controles existentes y la evaluación del riesgo residual que necesariamente debe ser gestionada a través de implementación de controles propuestos en el tratamiento de los riesgos.

Identificación y evaluación de controles Seguridad Digital:

Para los casos en los cuales se determine Reducir el Riesgo o Compartir el riesgo se deben estructurar controles que cumplan con las características establecidas en el presente documento.

- **Tipos De Controles**:

  - **Control preventivo:** buscan evitar que el evento de riesgo se materialice (disminuyen la probabilidad) y están orientados a atacar las causas que facilitan la materialización del evento de riesgo.

  - **Control detectivo**: buscan identificar la situación no deseada, una vez se haya presentado, y tiene por objetivo minimizar el impacto de la materialización del evento de riesgo, por eso este tipo de riesgo está encaminado a disminuir las consecuencias del riesgo.

Se propenderá estructurar un Control que permita dar cobertura de carácter preventivo y detectivo.

- Características de un control adecuadamente estructurado

Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo éste debe cumplir con los siguientes lineamientos:

- ✓ Debe tener un **responsable** de su ejecución (evitar colocar áreas generales o nombres propios), por ejemplo: responsable de inventarios.
- ✓ Cada causa del riesgo debe tener **por lo menos un control** asignado a su mitigación.
- ✓ La ejecución del control **debe tener un soporte documental**, por ejemplo, una base de datos, una lista de chequeo, un acta de reunión, etc.
- ✓ En la descripción del control se debe **especificar como se ejecuta** el control.
- ✓ En la definición del control se debe especificar cuál es la **periodicidad de la aplicación** de este; por ejemplo: el coordinador debe revisar (mensualmente, trimestralmente, cada vez que se presente)
- ✓ La definición debe incluir **cual es el propósito** del control (valida, coteja, compara, concilia…)
- ✓ La definición del control debe incluir en que situaciones se presentan **desviaciones entre el resultado esperado y el resultado obtenido** y que acciones se deben tomar si se presentan dichas desviaciones.

7.2.4. Metodología para el diseño de los controles

Para el establecimiento de los controles y establecer si éstos realmente apuntan a mitigar el riesgo y mitigan las causas para prevenir que el riesgo se materialice, se debe considerar para su diseño las siguientes variables[8]:

Paso 1. Definir el responsable de realizar la actividad de control.

Paso 2. Establecer la periodicidad para la ejecución de la actividad

Paso 3. Indicar el propósito del control

Paso 4. Indicar cómo se realiza la actividad de control

Paso 5. Establecer que pasa en caso de desviaciones u observaciones resultado de ejecutar el control.

Paso 6. Establecer y dejar evidencias de la ejecución del control.

[8] Tomado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

Descripción de los pasos:

Paso 1. Definir el responsable de realizar la actividad de control.

Para que el control cumpla, el responsable debe:

- Tener la autoridad, competencia y conocimiento para ejecutar la actividad de control dentro del proceso.
- Las responsabilidades deben estar segregadas o distribuidas entre diferentes personas para disminuir la concentración de funciones que generen errores o riesgo de corrupción.

- ✓ El control debe iniciar con un cargo responsable (manual) o un sistema o aplicación (automático)
- ✓ Evitar asignar áreas de manera general o nombres de personas.
- ✓ El control debe estar asignado a un cargo específico.

Paso 2. Establecer la periodicidad para la ejecución de la actividad

La periodicidad en la actividad de control debe:

- Tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.).
- Su ejecución debe ser consistente y oportuna para la mitigación del riesgo.

- ✓ Todas las actividades de control deben definir una periodicidad específica. (mensual, trimestral, semestral, etc.)
- ✓ En caso de controles automáticos, también tienen una periodicidad. (están programados)
- ✓ Si queda a criterio la periodicidad de la realización del control, se tiene un problema en el diseño del control.

Paso 3. Indicar el propósito del control

El control debe tener un propósito que indique para qué se realiza:

- El propósito debe conllevar a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar).
- Tener en cuenta si es un control o una actividad de control. (importante la redacción)
- Detectar la materialización del riesgo, para realizar los ajustes y correctivos en el diseño del control o en su ejecución.

✓ El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo.
✓ También aplica para los controles automáticos

Paso 4. Indicar cómo se realiza la actividad de control

El control debe tener el cómo se realiza:

- Debe indicar si la fuente u origen de la información que ejecuta el control es confiable para mitigar el riesgo.
- Cuando se evalúe el control debe permitir establecer la confiabilidad del mismo para mitigar su materialización.

✓ El cómo se puede realizar a través de listas de chequeo, cruces de validaciones automáticas frente a registros o información de usuarios o proveedores (cédula. NIT. valores. etc.)

Paso 5. Establecer qué pasa en caso de desviaciones u observaciones resultado de ejecutar el control.

El control debe indicar qué se debe hacer con las observaciones o desviaciones resultado de ejecutar el control.

- Si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación.
- Si es un control que detecta una posible materialización de un riesgo, se debe gestionar de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

✓ Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control no tiene el efecto para lo cual fue diseñado.

Paso 6. Establecer y dejar evidencias de la ejecución del control.

. Esta evidencia ayuda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo a la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control

✓ La evidencia debe permitir realizar verificaciones sobre la realización del control adecuadamente, por terceros. (auditorías, verificaciones)
✓ La evidencia puede ser física, digital o el registro que deja un control automático.

7.2.5. Evaluación de los controles.

Una vez se tengan identificados los controles o actividades de control, éstos deben ser evaluados, con el fin de que permitan minimizar la probabilidad o el impacto de los riesgos y poder establecer los riesgos residuales (riesgos calificados después de controles), permitiendo modificar los riesgos y desplazarlo de una zona a otra dentro de la Matriz de Evaluación.

La ART, adopta la metodología para la valoración de los controles de acuerdo con los lineamientos del DAFP dados a través de la Guía para la administración de riesgos y diseño de controles en entidades públicas (3.2.2. valoración de controles).

Para la adecuada mitigación de los riesgos:

- ✓ El control debe estar bien diseñado
- ✓ El control debe ejecutarse por parte de los responsables tal como se diseñó.
- ✓ Un control que esté bien diseñado y se ejecute adecuadamente, contribuye a la mitigación del riesgo.

Fuente. Adaptado de la Guía para la administración de riesgos y diseño de controles en entidades públicas DAFP

Aspectos a tener en cuenta para el análisis y evaluación de los controles[9]:

- Determinar la naturaleza del control si es preventivo o detectivo.

Preventivo: Previene que el evento suceda. Disminuye la probabilidad.

Detectivo: Permite controlar la situación en caso de materialización del riesgo. Disminuye el impacto.

- Establecer si el control se encuentra documentado, si tiene un responsable, frecuencia o periodicidad de seguimiento y si cuenta con registro de los seguimientos.

Teniendo en cuenta estos aspectos, la evaluación se realiza a cada uno de los controles identificados en cada riesgo, de acuerdo con el cuadro del Anexo 2 Evaluación de Controles, con el fin de determinar si cumplen con los aspectos de diseño y ejecución.

En los formatos para la Gestión de Riesgos de Procesos y los Riesgos de Seguridad Digital, se encuentran los campos para la evaluación de controles de acuerdo con la valoración dada por el DAFP, para cada uno de los componentes.

EVALUACIÓN DEL DISEÑO DEL CONTROL											
Responsable	VALOR	Segregación y autoridad del responsable	VALOR	Periodicidad del control	VALOR	Propósito del Control	VALOR	Como se realiza la actividad de control	VALOR	Que pasa con las observaciones y desviaciones	VALOR

Matriz de Riesgos Gestión y SD- 2020

Resultado de la evaluación del diseño de los controles:

RESULTADO EVALUACIÓN DEL DISEÑO	RANGO DE CALIFICACIÓN
FUERTE	Entre 96 y 100
MODERADO	Entre 89 y 95
DÉBIL	Entre 0 y 88

[9] **Tomado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4**

Si el resultado de la calificación del control o el promedio del *diseño* es menor de **96** puntos (MODERADO O DÉBIL), se debe establecer acciones que permita tener un control o controles bien diseñados.

Resultado de la evaluación de la ejecución de los controles:

Los controles también se deben ser evaluados respecto de la ejecución de los mismos por parte de los responsables, "no basta con que el control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo." [10]

EVALUACIÓN EJECUCIÓN Y SOLIDÉZ DEL CONTROL							
Evidencia de la ejecución del control	VALOR	CALIFICACIÓN DISEÑO DEL CONTROL		EVALUACIÓN EJECUCIÓN DEL CONTROL		SOLIDEZ DEL CONTROL	VALOR

Matriz de Riesgos Gestión y SD- 2020

RESULTADO EVALUACIÓN DE LA EJECUCIÓN DEL CONTROL	RANGO DE CALIFICACIÓN
FUERTE	**15** - El control se ejecuta de manera consistente por parte del responsable.
MODERADO	**10**- El control se ejecuta algunas veces por parte del responsable
DÉBIL	**0**- El control no se ejecuta por parte del responsable

7.2.6 Análisis y evaluación de controles para la mitigación de los riesgos.

La calificación tanto de los riesgos inherentes como residuales se realiza a los riesgos (no a las causas). Para establecer si los controles ayudan al tratamiento de los riesgos, se deben evaluar de manera individual o en conjunto, para lo cual se considera tanto la evaluación del diseño, como la ejecución y el promedio de los controles en su conjunto (para cada riesgo).

[10] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

Del resultado de esta evaluación se obtiene la SOLIDEZ del control y se establece SI se requiere o NO levantar acciones para fortalecer el control.

Para este ejercicio se cuenta con la matriz del Anexo 3 Solidez de controles, el cual genera el resultado de la solidez de cada control, de acuerdo con la calificación de la evaluación del diseño y ejecución del control.

SOLIDEZ DEL CONTROL			
PESO EJECUCIÓN DEL CONTROL	**PESO DISEÑO DEL CONTROL**		
	FUERTE Entre 96 a 100	**MODERADO** Entre 95 y 86	**DÉBIL** Entre 85 y 0
FUERTE Siempre se ejecuta	**FUERTE (100)**	**MODERADO (50)**	**DÉBIL (0)**
MODERADO Algunas veces se ejecuta	**MODERADO (50)**	**MODERADO (50)**	**DÉBIL (0)**
DÉBIL No se ejecuta	**DÉBIL (0)**	**DÉBIL (0)**	**DÉBIL (0)**

SOLIDEZ DEL CONTROL	SI/NO acciones para fortalecer el control	Calificación solidez del control
FUERTE	**NO**	**100**
MODERADO	**SI**	**50**
DÉBIL	**SI**	**0**

Fuente: Anexo 3 solidez de controles ART- 2020.

Para determinar la solidez del conjunto de controles para un determinado riesgo, teniendo en cuenta que un mismo riesgo pude tener varias causas y éstas a su vez uno o más controles, se requiere determinar la solidez del control en su conjunto, por lo que se hace necesario realizar dicho ejercicio primero individual y luego en su conjunto. (Ver matriz a continuación matriz evaluación de la solidez del control integral)

La solidez del conjunto resulta del promedio aritmético simple de los controles para cada riesgo así:

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE COTROLES	
FUERTE	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a **100**
MODERADO	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre **50 y 99**
DÉBIL	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es **menor que 50**

Anexo 3 Solidez de controles ART- 2020. (Adaptado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP)

7.2.7 Valoración de riesgos después de controles (riesgo residual)

Como resultado de la evaluación de los controles en forma integral, se realiza de nuevo la valoración del riesgo, con el fin de establecer su calificación y determinar el riesgo residual. (Riesgo después de controles), para tal fin se tiene en cuenta:

Desplazamiento del riesgo inherente para calcular el riesgo residual:

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente matriz:

MATRIZ DESPLAZAMIENTO RIESGO INHERENTE PARA CALCULAR RIESGO RESIDUAL						
Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir Impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de Impacto	Clase de Riesgo	Clase de controles
FUERTE	DIRECTAMENTE	DIRECTAMENTE	**2**	**2**	Gestión	Preventivos y detectivos
FUERTE	DIRECTAMENTE	INDIRECTAMENTE	**2**	**1**	Gestión	Preventivos
FUERTE	DIRECTAMENTE	No DISMINUYE	**2**	**0**	Corrupción	Preventivos **o** detectivos
FUERTE	No DISMINUYE	DIRECTAMENTE	**0**	**2**	Gestión	Detectivos
MODERADO	DIRECTAMENTE	DIRECTAMENTE	**1**	**1**	Gestión	Preventivos y detectivos
MODERADO	DIRECTAMENTE	INDIRECTAMENTE	**1**	**0**	Gestión	Preventivos
MODERADO	DIRECTAMENTE	No DISMINUYE	**1**	**0**	Corrupción	Preventivos **o** detectivos
MODERADO	No DISMINUYE	DIRECTAMENTE	**0**	**1**	Gestión	Detectivos
DÉBIL	No DISMINUYE	No DISMINUYE	**0**	**0**	Gestión y Corrupción	Preventivos y/o detectivos

Fuente: ART- 2019. Adaptado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP

De acuerdo con el resultado anterior, se determina el desplazamiento del riesgo ya sea en probabilidad o impacto, dentro del cuadrante del Anexo 4 Calificación de riesgos, estableciendo la calificación del riesgo residual, para establecer el tratamiento, según la zona donde haya quedado ubicado el riesgo.

7.4 Tratamiento o manejo de riesgos residuales

El tratamiento o manejo de riesgos, es el conjunto de medidas que se toman, con el fin de tratar los riesgos y mitigar su materialización a través de la toma de medidas o acciones para su mitigación.

Con base en el formato FM-DE-08 MATRIZ DE RIESGOS del Formato de Gestión de Riesgos, cada líder de proceso y el gestor(es), junto con su equipo de trabajo, de acuerdo con la calificación y la zona de riesgo que haya quedado ubicado el riesgo, establecen el tratamiento para cada uno, de conformidad con las Políticas de Administración adoptadas por la ART. (Ver numeral 6.1.2 del presente Manual y Anexo 5 Tratamiento de Riesgos de Gestión y Corrupción).

ANEXO 5. TRATAMIENTO DE LOS RIESGOS - ART			
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL			
CALIFICACIÓN	**POLÍTICA MANEJO RIESGO**	**PLAN DE MANEJO**	**PLAN CONTINGENCIA**
ZONA BAJA	**ASUMIR O ACEPTAR EL RIESGO**	Riesgos inhrentes, no se adoptan medidas que afecten la probabilidad o el impacto. Realizar monitoreos periódicos, al menos semestral o trimestralmente al riesgo y controles para que permanezcan en zona baja.	NA
ZONA MODERADA	**REDUCIR EL RIESGO**	Establecer acciones, medidas que permitan reducir la probabildiad y/o el impacto del riesgo. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.	NA
ZONA ALTA	**EVITAR EL RIESGO**	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. Monitoreo bimensual a los controles y acciones establecidas.	Es optativo establecer planes de contingencia, para aplicar en caso de que el riesgo se meterialice.
ZONA EXTREMA	**EVITAR EL RIESGO** **COMPARTIR O TRANSFERIR EL RIESGO**	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando tanto la probabilidad y/o impacto. Monitoreo mensual a los controles y acciones establecidas.	Establecer planes de contingencia para aplicar en caso de que el riesgo se meterialice.

RIESGOS DE CORRUPCIÓN			
ZONA BAJA ZONA MODERADA	REDUCIR EL RIESGO	Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad de ocurrencia. Monitoreos periódicos, mínimo cada trimestre a los controles y acciones.	N/A
ZONA ALTA ZONA EXTREMA	EVITAR EL RIESGO	Establecer acciones o medidas que busquen evitar la materialización del riesgo, mitigando la probabilidad de ocurrencia. Monitoreos bimensuales o mensuales a los controles y acciones establecidas	Establecer planes de contingencia para aplicar en caso de materialización

Fuente: ART-2020- Adaptado de la Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4.

7.4.1 Planes de Manejo para mitigar los riesgos.

En el Plan de Manejo de riesgos, se establecen las acciones o medidas a seguir de acuerdo con la zona y el nivel de aceptación de cada uno y de acuerdo con la solidez de los controles, con el fin de mitigar las causas generadoras de riesgos.

Para el establecimiento de las acciones se debe tener en cuenta:

- ✓ Los riesgos de GESTIÓN que permanezcan en Zona BAJA y los controles son FUERTES, no se requiere establecer Planes de Manejo.
- ✓ Para los riesgos que se encuentren en ZONA MODERADA, ALTA O EXTREMA, se debe establecer acciones que permitan evitar que el riesgo se materialice.
- ✓ Para los riesgos que presentan controles con solidez MODERADA O DÉBIL, independiente de la ZONA donde se encuentren, se les debe establecer acciones para fortalecer los controles.
- ✓ Los riesgos de CORRUPCIÓN, independiente de la zona donde se encuentren, se les debe establecer planes de manejo para evitar su materialización y mantener mitigado el riesgo.

Planes de Contingencia: Son planes de manejo para los riesgos que se les debe dar un tratamiento especial o se les establece generalmente, para los riesgos calificados en zona alta o extrema y se ponen en marcha, en caso de materialización del riesgo.

Este Plan de Manejo se registra en el formato FM-DE-08 Matriz de Riesgos, en el campo de PLAN DE MANEJO, el cual contiene:

- ✓ Las acciones para la mitigación de los riesgos.
- ✓ Los responsables de ejecutar las acciones
- ✓ La periodicidad de seguimiento de la acción, la cual depende de la zona donde se encuentre el riesgo. Puede ser mensual, bimestral o trimestral.
- ✓ Las fechas de inicio y finalización de las acciones.

PLAN DE MANEJO						
ACCIONES A TOMAR	PRODUCTO	RESPONSABLE	FECHA DE INICIO (dd/mm/año)	FECHA DE TERMINACIÓN (dd/mm/año)	PERIODICIDAD DE SEGUIMIENTO RIESGOS Y CONTROLES	PLANES DE CONTINGENCIA (si aplica)

FM-DE-08 MATRIZ DE RIESGOS- Plan de Manejo

7.4.2 Mapas de Riesgos

El mapa de riesgo es consolidado de los riesgos identificados en cada proceso, los riesgos residuales, planes de manejo y planes de contingencia. EL mapa es el resultado de la Matriz de Riesgos de cada proceso y cuenta con el Formato FM-DE-09 Mapa de Riesgos de Proceso y del formato FM-DE-22 de Gestión de Riesgos de SD.

El formato mapa de riesgos contiene:

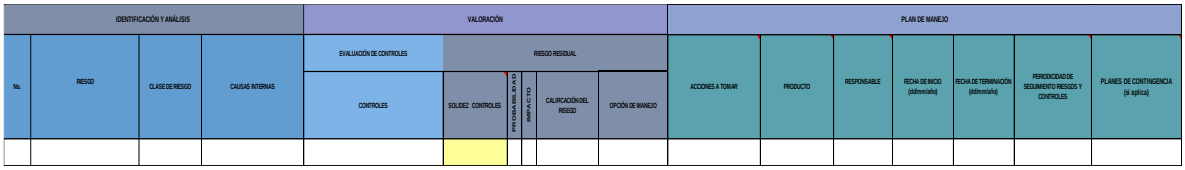
- IDENTIFIACIÓN DE RIESGOS
  - Número y Riesgo
  - Clase de Riesgo
  - Causas Internas

- VALORACIÓN
  Evaluación de Controles

- RIESGO RESIDUAL
  - Solidez de Controles
  - Probabilidad
  - Impacto

- Calificación del riesgo (después de controles)
- Opciones de manejo

- TRATAMIENTO O PLAN DE MANEJO
  - Acciones
  - Producto
  - Responsable
  - Fecha de inicio
  - Fecha de finalización
  - Periodicidad de seguimiento
  - Planes de Contingencia



IDENTIFICACIÓN Y ANÁLISIS				VALORACIÓN					PLAN DE MANEJO						
No.	RIESGO	CLASE DE RIESGO	CAUSAS INTERNAS	EVALUACIÓN DE CONTROLES	RIESGO RESIDUAL				ACCIONES A TOMAR	PRODUCTO	RESPONSABLE	FECHA DE INICIO (dd/mm/año)	FECHA DE TERMINACIÓN (dd/mm/año)	PERIODICIDAD DE SEGUIMIENTO RIESGOS Y CONTROLES	PLANES DE CONTINGENCIA (si aplica)
				CONTROLES	SOLIDEZ CONTROLES	PROBABILIDAD	IMPACTO	CALIFICACIÓN DEL RIESGO	OPCIÓN DE MANEJO						

FM-DE-09 MAPA DE RIESGOS-ART 2020

Los mapas de riesgos permiten llevar el control de los riesgos, a nivel de proceso y a nivel estratégico.

Los Mapas de Riesgo son consolidados por la Oficina de Planeación y se clasifican en:

Mapa de Riesgo de Proceso: El cual contiene los riesgos identificados en cada uno de los procesos. Estos mapas deben ser revisados por el Director, Subdirector, Jefe de Oficina, Coordinador de Grupo o Líder de Proceso; y deben ser aprobados por el Líder del Proceso.

Mapa de Riesgo de Corrupción: Consolida los riesgos de corrupción identificados en cada proceso y es consolidado por la Oficina de Planeación. El mapa cuenta con el Formato de FM-DE-14 Mapa de Riesgos de Corrupción-ART.

Mapa de Riesgo de Seguridad Digital: El cual contiene los riesgos identificados en cada uno de los procesos relacionados con los riesgos inherentes a los activos de información de cada proceso. Estos mapas deben ser revisados por el Director, Subdirector, Jefe de Oficina, Coordinador de Grupo o Líder de Proceso; y deben ser aprobados por el Líder del Proceso.

Mapa de Riesgo de Institucional: El cual consolida los riesgos identificados en cada proceso calificados *en zona alta y extrema y los riesgos de corrupción*. Este es consolidado por la Oficina de Planeación.

8. MONITOREO Y SEGUIMIENTO

8.1. Monitoreo de los mapas de riesgos.

El monitoreo a los mapas de riesgos es esencial para asegurar la eficiencia y eficacia de las acciones establecidas para el tratamiento de los riesgos de gestión, seguridad digital y de corrupción, la cual se adelanta a través del monitoreo, seguimiento y revisión periódica, de tal forma que permita evidenciar todas aquellas situaciones o factores que puedan influir en el resultado de las acciones.

El monitoreo a los mapas de riesgos, *la realizará los Líderes de Proceso*, con el apoyo de los gestores, de acuerdo con la periodicidad establecida en la Política de Administración de Riesgos y las responsabilidades establecidas, así:

Riesgos valorados en zona baja: Se debe realizar monitoreos periódicos, mínimo cada trimestre a los controles, para que permanezcan en esta zona o se pueda eliminar el riesgo.

Riesgos calificados zona moderada: Monitoreos periódicos, mínimo cada trimestre a los controles y acciones establecidas.

Riesgos calificados zona alta: Monitoreo bimensual a los controles y acciones establecidas.

Riesgos calificados zona extrema: Monitoreo mensual a los controles y acciones establecidas y se requieres realizar pruebas periódicas a los planes de contingencia.

Como resultado del monitoreo y la revisión, de los mapas de riesgo, se puede generar la actualización o modificación de los mapas, sus riesgos, causas, consecuencias, controles, tratamientos y los planes de manejo de cada uno de los riesgos.

8.2 Seguimiento a los mapas de riesgos.

La Oficina de Planeación, será quien apoye a la Entidad, en el seguimiento periódico a los Mapas de Riesgos, con el apoyo del responsable de seguridad digital, para los Mapas de Riesgos de SD.

El Grupo Interno de Trabajo de Control Interno de la ART, es el responsable de realizar el seguimiento a los mapas de riesgos, con la periodicidad que se establezca en el Programa de Auditoría Interna para cada vigencia, o cuando por cualquier circunstancia lo establezca el Comité Institucional de Control Interno de la ART.

Lo cual lo hace mediante la evaluación independiente al diseño y ejecución de los controles, dando prioridad a los riesgos de gestión con mayores niveles de riesgo.

Seguimiento Riesgos de Corrupción.

Para el caso de los riesgos de corrupción, el seguimiento y publicación, se realizará de acuerdo a lo establecido en la Estrategia para el PAAC-V2 y la metodología establecida en la Guía para la Administración de Riesgos y Diseño de Controles en entidades públicas del DAFP.

"El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- ✓ Verificar la publicación del Mapa de Riesgos de Corrupción en
- ✓ la página web de la entidad.
- ✓ Seguimiento a la gestión del riesgo.
- ✓ Revisión de los riesgos y su evolución.
- ✓ Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Fechas de seguimientos y publicación:

El seguimiento se realiza tres (3) veces al año, así:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10), primeros días hábiles del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero" [11].

Para el seguimiento de los riesgos de corrupción, se podrá utilizar el formato del Anexo 6 Matriz de seguimiento a los riesgos de corrupción de la Guía del DAFP.

8.3 Reporte resultado del monitoreo y seguimiento

Cuando se determine que se los mapas de riesgo deben ser modificados, como resultado del monitoreo que realicen los líderes de proceso, como resultado del seguimiento que realice el Grupo de Control Interno, o los diferentes Entes de Control, se debe:

[11] Guía para la administración de riesgos y diseño de controles en entidades públicas. DAFP-2018 V4

- ✓ Reportar a la Oficina de Planeación, con el fin de actualizar los mapas correspondientes, en cualquiera de sus componentes, ya sea a los riesgos, sus causas, consecuencias, controles, tratamientos o planes de manejo.

- ✓ Si se identifican cambios internos o externos que puedan impactar positiva o negativamente a la Entidad o algún proceso, se reporta a la Oficina de Planeación, con el fin de apoyar la identificación, análisis y valoración de riesgos de gestión o corrupción del proceso.

- ✓ Los reportes que se hagan a la Oficina de Planeación se deben realizar a través de correo electrónico, soportado con la Matriz de Riesgos de Gestión y de SD y el acta de reunión resultado del monitoreo o el resultado del seguimiento del Grupo Interno de Control Interno.

Cuando se realice el *monitoreo de los riesgos de corrupción*, se debe reportar el resultado de este a la Oficina de Control Interno según las fechas que ésta determine y de acuerdo a los cortes cuatrimestrales establecidos en el numeral 8.1 del presente manual, concordante con la Guía para la Gestión del Riesgo de Corrupción-2015.y a la Oficina de Planeación.

- ✓ La Oficina de Planeación, será la encargada de consolidar el Mapa de Riesgos Institucional y presentar al Comité de Institucional de Gestión y Desempeño y/o al Comité de Coordinación de Control Interno el resultado del monitoreo y seguimiento que se realice a los mismos, con el fin de establecer la necesidad de definir si es necesario la revisión y ajuste de la Política de Administración de Riesgos de la Agencia o se deba tomar acciones sobre riesgos estratégicos, de SD o de corrupción que presenten una alta probabilidad de materializarse.

- ✓ Si se detecta la materialización de un riesgo ya sea de gestión, SD o corrupción, se debe informar a las instancias respectivas, de acuerdo con lo establecido en el numeral 6.1.3. del presente Manual**,** relacionado con el "Tratamiento a los riesgos materializados."

9. SOCIALIZACIÓN Y COMUNICACIÓN

La comunicación y divulgación de la política y la metodología para la administración de los riesgos, será dada a conocer por la Oficina de Planeación, en coordinación con la Oficina de Comunicaciones, la cual se realizará a través de los diferentes medios de comunicación interna, con el fin de dar cubrimiento al mayor número de servidores públicos de la Entidad, tanto a nivel central, como a nivel territorial.

Así mismo, los líderes de proceso con el apoyo de los gestores socializarán la política y los mapas de riesgos a los equipos de trabajo, así como los cambios y actualizaciones que se llegaran a generar, dejando registro de las mismas.

10. CONTROL DE CAMBIOS

Cuando se requiera modificar o actualizar el Manual de Administración de Riesgos, en relación con la política, la metodología para la gestión de riesgos, lo realizará la Oficina de Planeación y se presentará en el Comité Institucional de Control Interno, para ser aprobado por parte del Representante Legal de la ART, de conformidad con el literal g del artículo 2.2.21.1.6 del Decreto 1083 de 2015. (Funciones del Comité)

> "*Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta"*

La actualización, modificación, ajuste y publicación del Manual estará a cargo de la Oficina de Planeación y se publicará con las versiones actualizadas en el repositorio MERCURIO/SIGART.

Las modificaciones o actualización de versiones al Manual, sus anexos y formatos para la gestión de riesgos, que no impliquen cambios en la política y metodología serán realizadas por la Oficina de Planeación, cuando así se requiera y publicadas con las versiones actualizadas, en el repositorio Mercurio/SIGART.

ANEXO 1.

CONTROLES DE SEGURIDAD DIGITAL: Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece			
Número	**Nombre**	**seleccionado / Excepción**	**Descripción y/o Justificación**
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5. Políticas de seguridad de la información			
.5.1	Directrices establecidas por la dirección para la seguridad de la información		Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información		Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información		Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6 . Organización de la seguridad de la información			
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

A.6.1.1	Roles y responsabilidades para la seguridad de información		Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial		Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles		Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 . Seguridad de los recursos humanos			
A.7.1	Antes de asumir el empleo		Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección		Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

A.7.1.2	Términos y condiciones del empleo		Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección		Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario		Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo		Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir. A
A.8 Gestión de activos			
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos		Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos		Control: Los activos mantenidos en el inventario deberían tener un propietario.

A.8.1.3	Uso aceptable de los activos		Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos		Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información		Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información		Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información		Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos		Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles		Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios		Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos		Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9 Control de acceso			
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso		Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

A.9.1.2	Política sobre el uso de los servicios de red		Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información		Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

A.9.4.2	Procedimiento de ingreso seguro		Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas		Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados		Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas. A
A.10 Criptografía			
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos		Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves		Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11 Seguridad física y del entorno			
A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física		Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada		Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

A.11.1.4	Protección contra amenazas externas y ambientales		Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos		Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro		Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado		Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos		Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos		Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos		Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.

A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones			
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados		Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	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.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	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.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos		Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. A.12.3 Copias de respaldo Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información		Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. A.12.4 Registro y seguimiento Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes		Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos		Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas		Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software		Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas		Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones			
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes		Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

A.13.1.2	Seguridad de los servicios de red		Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información		Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información		Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información		Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica		Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimientos de sistemas			
A.14.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas		Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro		Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas		Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros		Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro		Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente		Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas		Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

A.14.2.9	Prueba de aceptación de sistemas		Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados. A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba		Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15 Relación con los proveedores			
A.15.1	Seguridad de la información en las relaciones con los proveedores		Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores		Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

A.16 Gestión de incidentes de seguridad de la información			
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos		Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información		Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información		Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información		Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia		Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

A.17.1.1	Planificación de la continuidad de la seguridad de la información		Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información		Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
A.17.2	Redundancias		Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18 Cumplimiento			
A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual		Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

A.18.1.3	Protección de registros		Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales		Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos		Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	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, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico		Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información