MANUAL- POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

AGENCIA DE RENOVACIÓN DEL TERRITORIO - ART

OFICINA DE PLANEACIÓN

Bogotá D.C.

Abril 2021

Versión 5

JUAN CARLOS ZAMBRANO ARCINIEGAS
Director General Agencia de Renovación del Territorio

ANDREA PAOLA FERNÁNDEZ GUARÍN
Jefe Oficina de Planeación

FREDY ALEJANDRO AGUAS
Profesional-
Oficina de Tecnologías de la Información

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; en octubre 14 del 2020, el Comité aprueba las modificaciones al Manual, donde se incluye la Política y metodología para los riesgos de Seguridad Digital, como parte integral de la gestión de riesgos de la ART, 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, permitiendo 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, esta actualización se

Teniendo en cuenta que el en diciembre del 2020, el Departamento Administrativo de la Función Pública-DAFP, modificó la metodología para la Gestión de Riesgos para las entidades públicas, se hace necesario ajustar y modificar la metodología para la gestión de riesgos de la Agencia, conforme a los nuevos lineamientos del DAFP.

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.” V.5-2020 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–Política de Administración de Riesgo de la Agencia de Renovación del Territorio-ART, tiene como objetivo establecer los lineamientos para el adecuado tratamiento, manejo y seguimiento de los riesgos, de gestión, corrupción y de seguridad digital a los que está expuesto la Entidad en el marco de sus actuaciones, para controlar las situaciones adversas que puedan impactar el cumplimiento de los objetivos estratégicos y misión institucional.

2. ALCANCE

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

Para los riesgos de gestión y corrupción, 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. V.5. diciembre de 2020. Departamento Administrativo de la Función Pública.

Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas- Anexo 4- DAFP. Agosto 2019

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.

Protocolo Identificación Riesgos corrupción Tramites- Anexo 3-DAFP diciembre 2018.

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, del Departamento Administrativo de la Función Pública- DAFP (Página 12 y 13) y del Anexo 4-Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

Activo de información: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Actividad 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: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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 permite reducir o mitigar un riesgo.

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

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

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. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por eficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la Infraestructura o por la ocurrencia de acontecimientos externos.

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: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

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.*
Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
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, el modelo de operación por procesos, misión; visión; objetivos estratégicos y la identificación 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. Articular procesos intersectoriales e intrasectoriales que garanticen intervenciones integrales que contribuyan al cierre de brechas rural-urbano y la transformación de los territorios priorizados, a través de la estructuración y ejecución de proyectos, la puesta en marcha de alternativas de desarrollo y el fortalecimiento de capacidades institucionales y comunitarias de manera sostenible en el marco de la implementación de los

Visión. En 2035 se habrán estabilizado los territorios intervenidos, a través de la implementación de los PDET y de los modelos de sustitución voluntaria de cultivos ilícitos, por lo que contarán con capacidades de autogestión, integrándose al desarrollo del país con equidad y legalidad

5.3 Objetivos estratégicos

La ART, reformuló los objetivos estratégicos y determinó nueve (9) objetivos, como base para el desarrollo y cumplimiento de la misión Institucional. Estos son:

Objetivo Estratégico 1: Coordinar y gestionar con los actores pertinentes a nivel nacional, territorial, públicos, privados y de cooperación internacional para la implementación de las iniciativas resultantes de los PATR y PISDA en zonas priorizadas

Objetivo Estratégico 2: Implementar estrategias para la gestión de recursos con entidades territoriales, nacionales, privadas y de cooperación internacional que permitan la financiación y cofinanciación de proyectos encaminados a la implementación de los Programas de Desarrollo con Enfoque Territorial- PDET.

Objetivo Estratégico 3: Implementar estrategias para el fortalecimiento de capacidades territoriales, de manera coordinada con las entidades competentes, con los gobiernos y autoridades locales y con los actores estratégicos territoriales para contribuir a la estabilización de zonas priorizadas.

Objetivo Estratégico 4: Implementar estrategias que promuevan la estructuración y ejecución de proyectos de ordenamiento social de la propiedad, desarrollo económico, social, ambiental, infraestructura y hábitat, así como de reconciliación en las zonas priorizadas.

Objetivo Estratégico 5: Diseñar e Implementar modelos de sustitución de cultivos de uso ilícito en aquellos territorios que para el efecto determine el Consejo Directivo de la ART

Objetivo Estratégico 6: Diseñar e implementar el modelo de gobierno de información para la producción y administración de información asociada con la implementación de los PDET y consolidar el banco de proyectos de inversión.

Objetivo Estratégico 7: Diseñar e implementar los mecanismos de seguimiento, monitoreo y evaluación asociados a la implementación de los PDET, que permitan orientar la toma de decisiones frente a los resultados esperados mediante el uso de herramientas de análisis de datos y ejercicios de prospectiva.

Objetivo Estratégico 8: Implementar un plan estratégico de pedagogía, divulgación y posicionamiento, que visibilice las transformaciones en los territorios priorizados, genere sentido de pertenencia, y promueva la irreversibilidad de los PDET.

Objetivo Estratégico 9: Garantizar una gestión efectiva que responda a las necesidades de los usuarios y/o ciudadanos internos y externos con altos estándares de calidad

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 de proyectos
- Articulación Nación-Territorio
- Información y prospectiva
- Sustitución de Cultivos ilícitos

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

Mediante Resolución N°000586 del 23 de octubre, se actualiza el Modelo de Operación por Procesos de la Agencia de Renovación del Territorio-ART y se deroga la Resolución 000893 de 2017.

El modelo de operación por procesos se encuentra alineado al Modelo Integrado de Planeación y Gestión, permitiendo el cumplimiento de los objetivos y misión institucional, el Mapa de Procesos está conformado por los siguientes procesos:

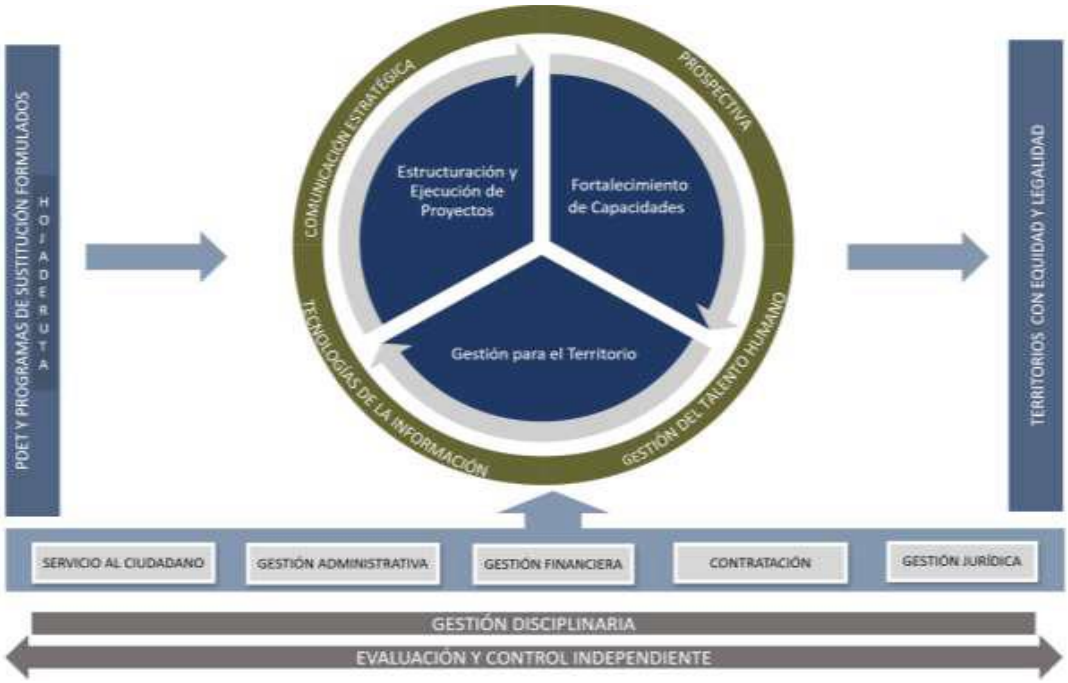
Estratégicos:
Prospectiva
Gestión de Talento Humano
Tecnologías de la Información
Comunicación Estratégica

Misionales
Gestión para el Territorio
Estructuración y Ejecución de Proyectos
Fortalecimiento de Capacidades

Apoyo
Servicio al ciudadano
Gestión Administrativa
Gestión Financiera
Contratación
Gestión Jurídica

Evaluación
Gestión Disciplinaria
Evaluación y Control Independiente

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



Fuente: Información Agencia de Renovación del Territorio-ART

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, 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.

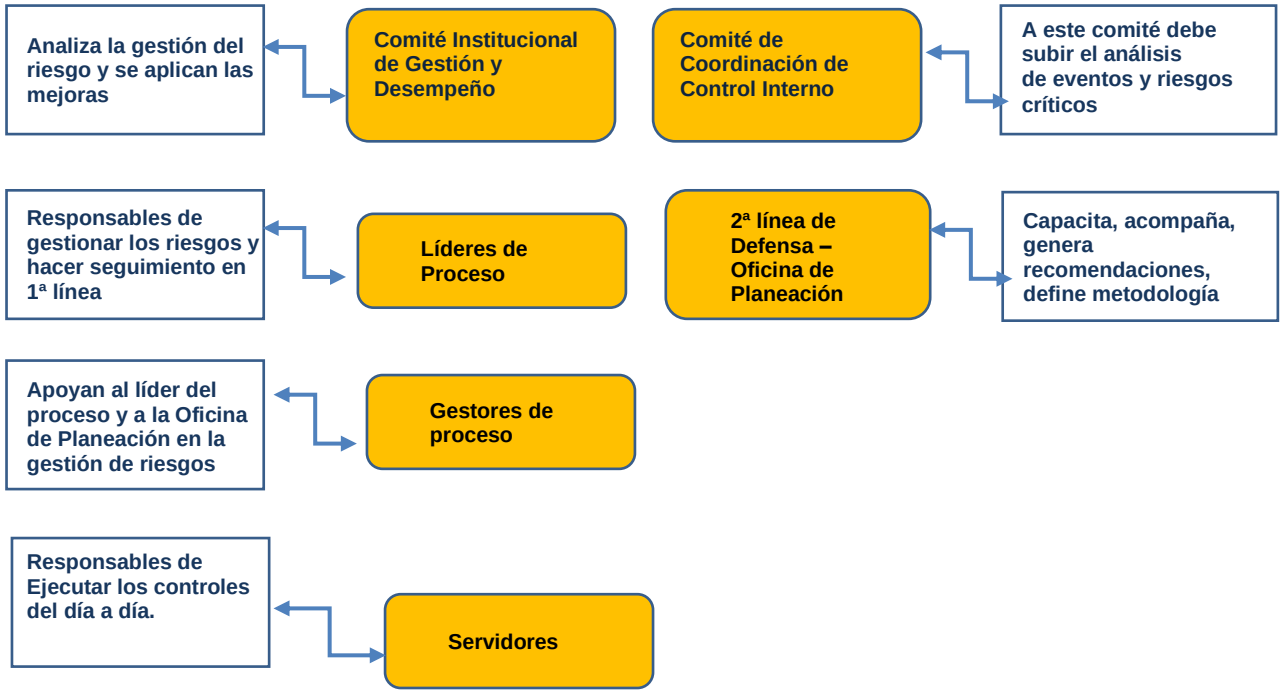
6. ASPECTOS GENERALES

Antes de iniciar con la metodología para la gestión de riesgos, se hace necesario tener en cuenta que la Agencia de Renovación del Territorio, en el marco del Modelo Integrado de Planeación y Gestión-MIPG, integra en la Política de Planeación Institucional, la Administración de riesgos, como parte de la Planeación Estratégica y es la línea Estratégica, la que define la Política de Administración de Riesgos, la cual es aprobada por parte del Comité de Coordinación de Control Interno.

El Comité Institucional de Gestión y Desempeño de la ART, se encuentra establecido mediante Resolución No.000142 del 20 de abril del 2018, modificado por la Resolución No.00585 del 23 de octubre del 2020, es la instancia encargada de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión en la Entidad y contempla las políticas de gestión y desempeño, conforme a las establecidas por el DAFP, mediante Decreto 1499 del 2017.

De conformidad con lo anterior, la ART, tiene en cuenta en la operatividad del MIPG, la gestión del riesgo, a través de las políticas del modelo y establece la metodología conforme a los lineamientos establecidos por el DAFP, a través de la Guía de Administración de Riesgos y el diseño de controles en entidades públicas-V.5- diciembre 2020.

Institucionalidad para la gestión de riesgos.

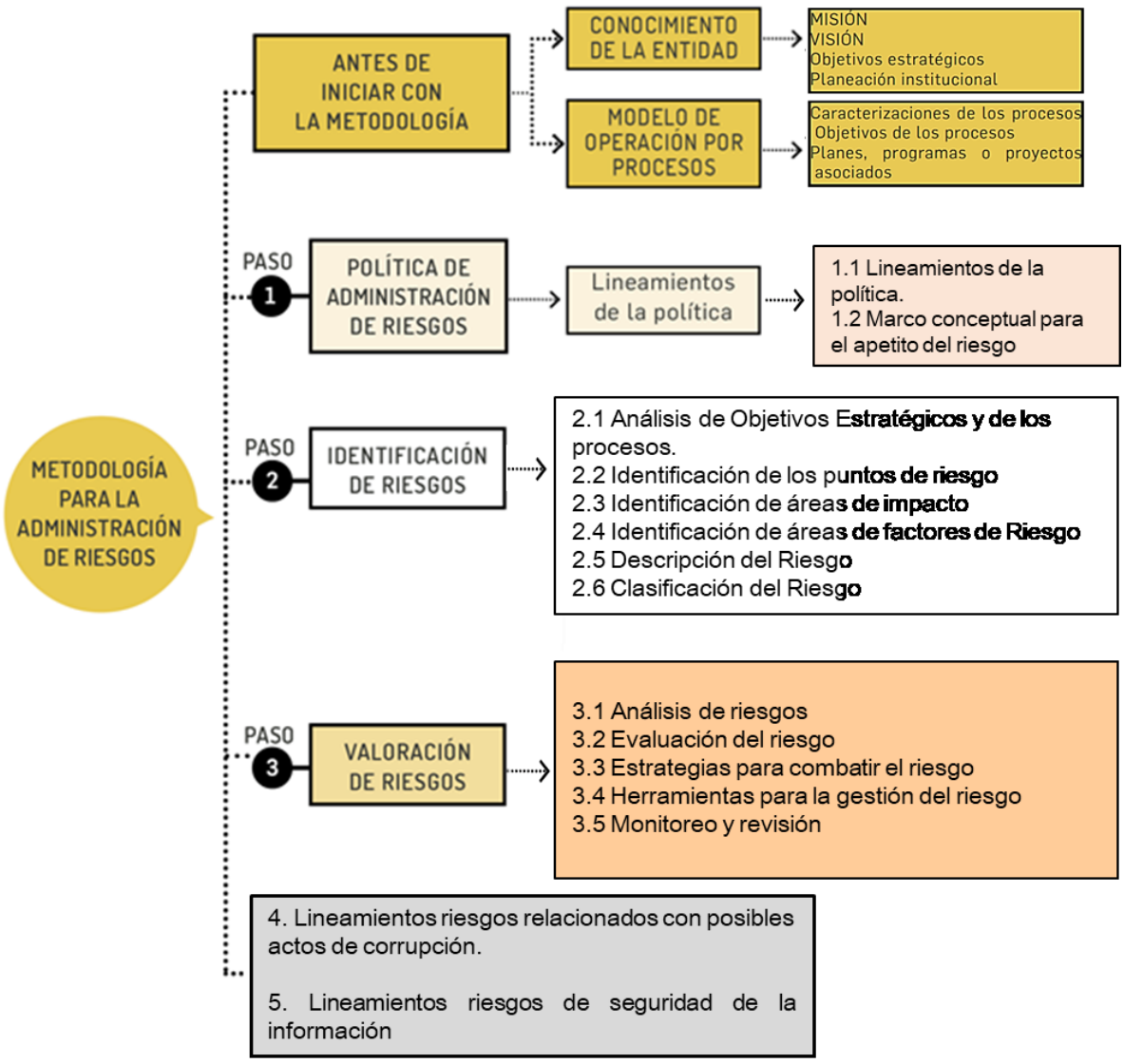


Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

La 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-V.5-2020 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 de gestión y corrupción



Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

Esquema para la Gestión de riesgos Digitales

La metodología para la gestión de los riesgos de Seguridad Digital se basa en la metodología establecida en el Modelo de Seguridad y Privacidad de la Información -MSPI del DAFP (Anexo No.4**)** y el Ministerio de Tecnologías de la Información y las Comunicaciones-MINTIC.

Herramienta para la gestión de riesgos

La Agencia de Renovación del Territorio-ART, adopta la matriz dada por el DAFP, de conformidad con el esquema para la gestión de riesgos y la metodología del DAFP.

De acuerdo con lo anterior, el formato de mapa de riesgos adoptado por la Entidad se encuentra controlado con el formato **FM-PS-DE-09**, para la identificación; análisis; evaluación de riesgos y valoración de controles; evaluación del riesgo residual; planes de manejo con sus respectivos campos, para los riesgos de gestión y corrupción.

Para la gestión de los riesgos de Seguridad Digital-RSD, se estructuró la matriz para la identificación y el análisis de los riesgos inherentes; valoración de los controles y planes de manejo con sus respectivos campos con el formato **FM-PS-DE-10**, bajo los parámetros de la Guía de Administración de Riesgos del DAFP y la guía Modelo de Seguridad y Privacidad de la Información -MSPI del DAFP (Anexo No.4**).**

Los formatos para al gestión de riesgos, se deben diligenciar acorde con el instructivo que contiene cada formato.

Clases de Mapas

El mapa de riesgo por procesos FM-PS-DE-09, 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 Seguridad Digital-RSD, FM-PS-DE-10, estará bajo la responsabilidad del responsable de seguridad digital, será consolidado por la Oficina de Tecnologías de la Información y publicado en Mercurio/SIGART, por la Oficina de Planeación. Este mapa 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 estará 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 enlace 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. 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, comunicación y control, que permitan el cumplimiento de los objetivos estratégicos 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 eventos de 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.

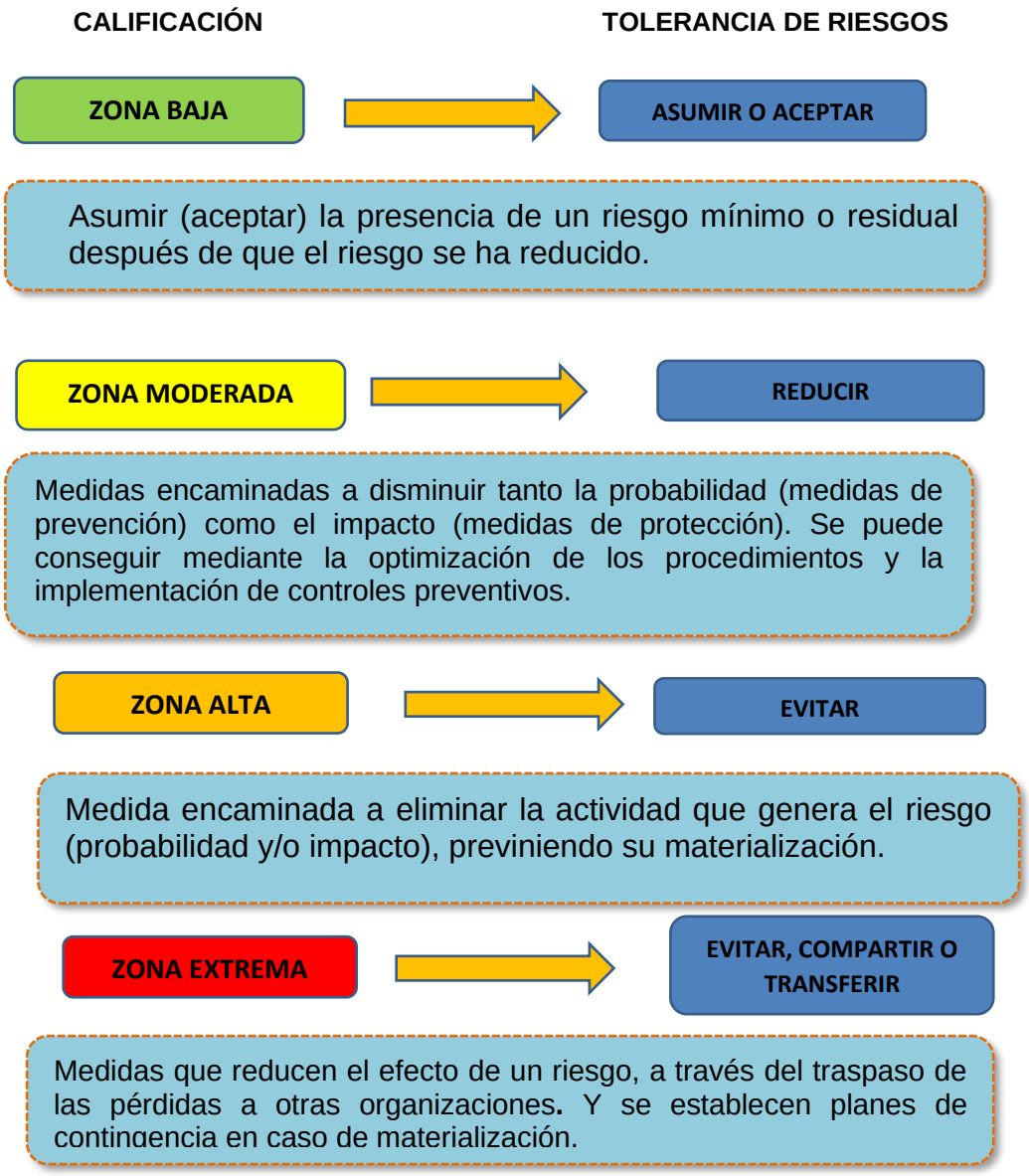
7.1 TOLERANCIA DE LOS RIESGOS.

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

7.1.1 La 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.

7.1.2 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 8.2 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 (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.

ZONA EXTREMA	COMPARTIR O TRANSFERIR EL RIESGO	Monitoreos bimensuales o mensuales a los riesgos y los controles. Establecer planes de contingencia para aplicar en caso de materialización.

Fuente: Agencia de Renovación del Territorio- ART 2019

7.1.3 Tratamiento a los riesgos materializados- eventos de riesgos.

En caso de materialización de los riesgos o eventos de 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: ART-2021

7.1.4 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 Instituciona 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:

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

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

8. 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-V.5 2020 del DAFP, el Modelo de Seguridad y Privacidad de la Información -MSPI del DAFP (Anexo No.4**)** 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.

8.1 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 estratégicos y 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.

8.1.1. Contexto estratégico.

La identificación del riesgo debe ser un proceso permanente, 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 estratégicos.

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.

8.1.2. Identificación de los puntos críticos

Para la identificación de los riesgos de proceso, se debe tener en cuenta las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo·.[2]

[2] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

Es importante que se analice la secuencia de los procesos y la cadena de valor, lo cual permite identificar los puntos críticos y el establecimiento de las actividades que pueden generar riesgo para el cumplimiento de los objetivos de los procesos de la Entidad. (mapa de procesos)

8.1.3. Identificación de las áreas de impacto.

De conformidad con la metodología establecida por el DAFP, se debe identificar las áreas de impacto, estas son: "la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional." .[3]

8.1.4. Identificación de las áreas de factores de riesgos.

Estas hacen referencia a la identificación de las fuentes generadoras de riesgos que pueda tener la Entidad, a nivel interno y externo.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
PROCESO	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	• Falta de procedimientos • Errores de registro, grabación, autorización • Errores en cálculos para pagos internos y externos • Falta de capacitación, temas relacionados con el personal
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	• Hurto de activos • Posibles comportamientos no éticos de los empleados • Fraude interno (corrupción, soborno)
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	• Daño de equipos • Caída de aplicaciones • Caída de redes • Errores en programas
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	• Derrumbes • Incendios • Inundaciones • Daños a activos fijos
EVENTOS EXTERNOS	Situaciones externas que afectan la entidad.	• Suplantación de identidad • Asalto a la oficina • Atentados, vandalismo, orden público • Fuerza mayor o caso fortuito

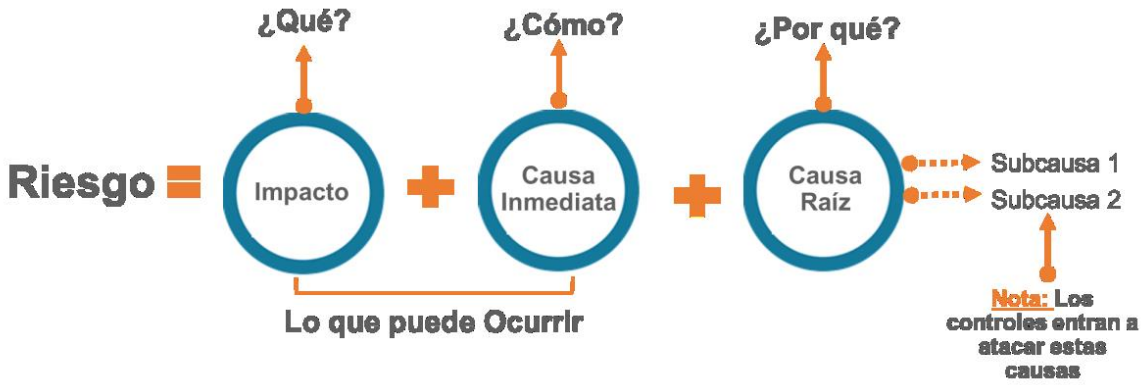
Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

[3] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

8.1.5 Descripción del riesgo.

Para la describir o redactar el riesgo en forma adecuada, de tal forma que permita una interpretación adecuada, se debe tener en cuenta:

Iniciar con la palabra **"POSIBILIDAD**" y seguidamente, analizar los siguientes aspectos:



Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

Es necesario identificar la causa inmediata (cómo) y la causa raíz (por qué), con el fin de que el riesgo quede bien identificado y su descripción evite interpretaciones subjetivas.

- ✓ **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ **Causa inmediata**: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- ✓ **Causa raíz**: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para tener en cuenta en la redacción del riesgo:

- **No** describir como riesgos omisiones ni desviaciones del control.
- **No** describir causas como riesgos.
- **No** describir riesgos como la negación de un control.
- **No** existen riesgos transversales, lo que pueden existir son causas transversales.

8.1.6. Clasificación y factores de Riesgo.

Para establecer una adecuada clasificación de los riesgos identificados se tienen la siguiente tipología, asociados a los procesos así:[4]

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Fraude externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno: Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos/eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

[4] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

Para la identificación de los riesgos, se hace necesario tener en cuenta los factores de riesgos:

CLASIFICACIÓN	FACTORES DE RIESGOS
Ejecución y administración de procesos	Procesos
Fraude externo	Eventos externos
Fraude interno	Talento Humano
Fallas tecnológicas	Tecnología
Relaciones laborales	Se asocian a varios factores
Usuarios, productos y prácticas	Se asocian a varios factores
Daños a activos fijos/eventos externos	Infraestructura- Evento externo

Fuente: Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

8.2. Valoración de los Riesgos

La valoración de riesgos consiste en establecer la probabilidad de ocurrencia del riesgo y nivel de consecuencia del impacto, con el fin de estimar la zona de riesgo inicial- RIESGO INHERENTE.[5]
Los elementos que se deben tener en cuenta para realizar la valoración son:

El análisis del riesgo: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial o riesgo inherente.

Evaluación de riesgos: Se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o riesgo residual.

8.2.1. Análisis de riesgos.

La construcción de los riesgos se realiza a partir de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

8.2.1.1 Determinación de la probabilidad.

La probabilidad o posibilidad de ocurrencia del riesgo, está asociada a la exposición del riesgo del proceso que se encuentra en análisis.

- ***La probabilidad inherente es el número de veces o frecuencia que se repite la actividad en un año***
- ***La exposición al riesgo estará asociada al proceso o actividad que se esté analizando***

[5] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

Criterios para definir el nivel de probabilidad

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**20%**
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**40%**
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**60%**
ALTA	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5000 veces por año.	**80%**
MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	**100%**

Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

8.2.1.2. Determinación del Impacto.

Para establecer el impacto de los riesgos identificados, se toman las variables de IMPACTO ECONÓMICO y REPUTACIONAL, lo que permite que la evaluación del riesgo sea más objetiva.

En el caso de que se presenten ambas variables, se toma la que presente el mayor nivel más alto.

Criterios para definir el nivel de impacto.

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
LEVE 20%	Afectación menor a 10 SMLV	El riesgo afecta la imagen de algún área de la organización.
MENOR 40%	Afectación entre 10 y 50 SMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
MODERADO 60%	Afectación entre 50 y 100 SMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
MAYOR 80%	Afectación entre 100 y 500 SMLV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
CATASTRÓFICO 100%	Afectación mayor a 500 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

- ***El líder del proceso será quien determine los criterios de probabilidad e impacta para el análisis del riesgo, que es quien conoce el proceso.***

8.2.2. Evaluación de los Riesgos

A partir del análisis de probabilidad e impacto, se establece la zona inicial que queda ubicado el riesgo inherente, en la tabla de calor.

Esta se determina mediante la combinación de la probabilidad y el impacto así:

MATRIZ CALIFICACIÓN DE RIESGOS					
Muy Alta 100%	ALTA	ALTA	ALTA	ALTA	EXTREMA
Alta 80%	MODERADA	MODERADA	ALTA	ALTA	EXTREMA
Media 60%	MODERADA	MODERADA	MODERADA	ALTA	EXTREMA
Baja 40%	BAJA	MODERADA	MODERADA	ALTA	EXTREMA
Muy Baja 20%	BAJA	BAJA	MODERADA	ALTA	EXTREMA
PROBABILIDAD	LEVE 20%	MENOR 40%	MODERADO 60%	MAYOR 80%	CATASTRÓFICO 100%
	IMPACTO				

Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

Como resultado de la evaluación los riesgos inherentes, se pueden ubicar en las siguientes zonas:

BAJO	
MODERADO	
ALTO	
EXTREMO	

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 estos, permitiendo establecer el riesgo residual (después de controles).

8.3. Valoración de los Controles

El control se define como la medida que permite reducir o mitigar el riesgo, para lo cual se debe tener en cuenta: [6]

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su qué hacer.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo

De acuerdo con la tipología de los controles se clasifican en:

Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen pueden generar costos implícitos.

De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

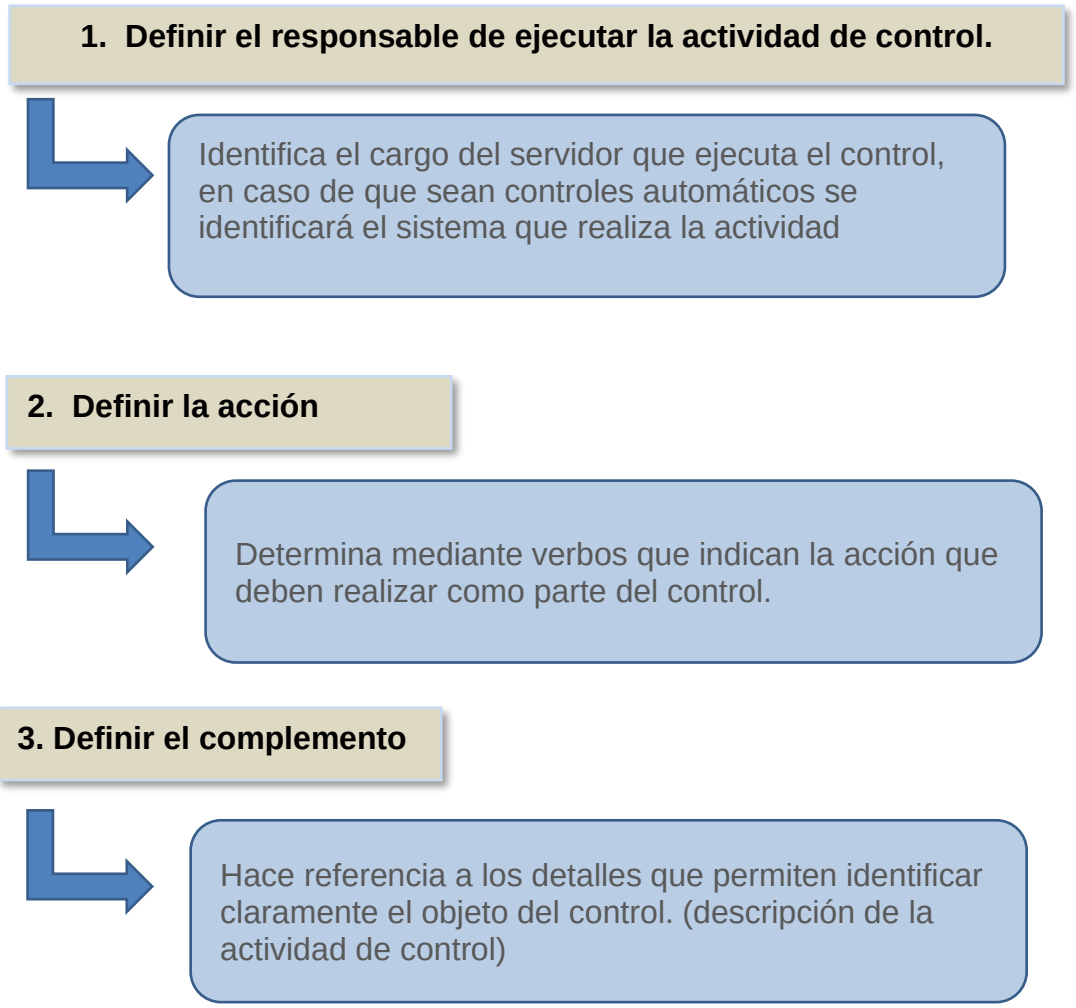
Las actividades de control tienen como fin:

TIPO DE CONTROL	RESULTADO	ETAPA DEL PROCESO
Controles Preventivos	Va a las causas del riesgo Atacan la probabilidad de ocurrencia del riesgo	**Entradas**
Controles Detectivos	Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo	**Ejecución de actividades**
Controles Correctivos	Atacan el impacto frente a la Materialización del riesgo	**Salidas**

[6] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

8.3.1. Estructura de los Controles

El DAFP, en la Guía de Administración de Riesgos y diseño de controles, establece la siguiente estructura para la valoración de los controles, la cual parte de la metodología anterior, así:



8.3.2. Diseño de los Controles

A continuación, se presenta la metodología, para el diseño, análisis y evaluación de los controles asociados a los riesgos, lo cual permitirá establecer el riesgo residual y su tratamiento.

Atributos para el diseño de los controles.

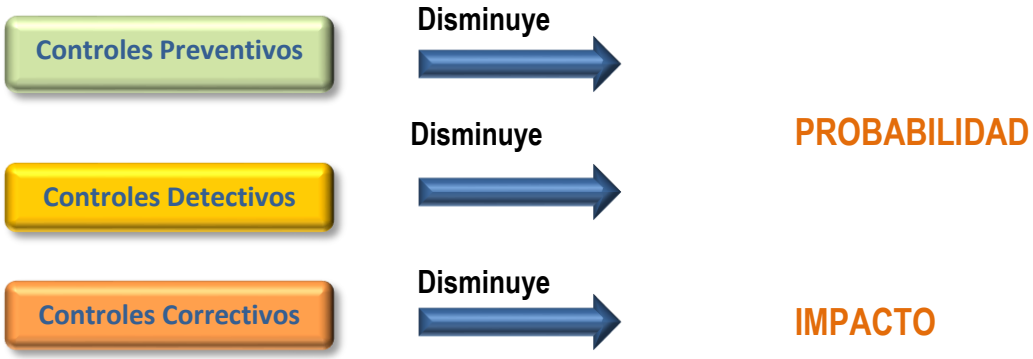
Para el diseño de los controles, se tienen en cuenta dos clases de atributos: Atributos de eficiencia y Atributos informativos.

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
TOTAL VALORACIÓN CONTROL				90%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

Fuente: Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

Los atributos de eficiencia dan una evaluación al control cuantitativa, lo cual permite determinar la efectividad del control y establecer la evaluación final del riesgo, al moverse en la matriz de calor (riesgo residual), de acuerdo con el tipo de control y disminuir la probabilidad o el impacto.

Los atributos informativos, sólo dan formalidad al control, permitiendo conocer el entorno del control de forma cualitativa, estos no generan calificación en la evaluación del control.



Nivel de riesgo residual.

Este se obtiene de aplicar la efectividad de todos los controles al riesgo inherente.

> Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.[7]

Para la identificación, valoración de controles se cuenta con la Matriz Mapa de Riesgo **FM-PS-DE-09,** la cual se adoptó del formato del DAFP, anexo de la Guía de Administración de Riesgos y establecimiento de controles V.5-2020.

Este formato se encuentra parametrizado y el cual genera la calificación del riesgo residual de conformidad con la clase de control, evaluación de sus atributos y generación del resultado final de acuerdo con la evaluación final de los controles que se identifiquen para cada riesgo.

Evaluación del riesgo - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual					
No. Control	Descripción del Control	Afectación	Atributos						Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
			Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia						
1		Probabilidad	Detectivo	Manual	30%	Sin Documentar	Continua	Con Registro	Baja	28%	Leve	20%	Bajo	Aceptar

8.4. Tratamiento 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-PS-DE-09** Mapa 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.

[7] **Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5**

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	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	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 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 controles y acciones establecidas	Establecer planes de contingencia para aplicar en caso de materialización
ZONA EXTREMA			

Fuente: Agencia de Renovación del Territorio-ART-2021

8.4.1 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, no se requiere establecer Planes de Manejo, se debe llevar un monitoreo periódico, para evitar su materialización
- ✓ Para los riesgos que se encuentren en ZONA MODERADA, ALTA O EXTREMA, se debe establecer acciones que permitan evitar que el riesgo se materialice.
- ✓ Los riesgos de CORRUPCIÓN, independiente de la zona donde se

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-PS-DE-09** Mapa 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
- ✓ Las fechas de inicio y finalización de las acciones.
- ✓ Los seguimientos a las mismas
- ✓ El estado

Plan de Manejo						
Plan de Acción	Responsable	Fecha de Inicio dd/mm/año	Fecha de finalización dd/mm/año	Fecha Seguimiento dd/mm/año	Seguimiento	Estado

Fuente: ART-2021 Adoptado- Adaptada de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

8.5. 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"[8].

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.

Una vez se haya realizado el ejercicio de la identificación de riesgos de corrupción, en el formato **FM-PS-DE-09 Mapa de Riesgos**, se registran los riesgos identificados, correspondiente a cada proceso, se clasifican de acuerdo con tipo de riesgo que pertenezca; en este caso ***fraude interno o fraude externo***.

8.5.1. Valoración de los riesgos de corrupción

Determinación de la probabilidad.

Para la valoración de los riesgos de corrupción, se determina la probabilidad de acuerdo con la metodología establecida para los riesgos de gestión, descrita en el numeral 8.2.2 del presente manual y se clasifican, según la tabla de frecuencia y probabilidad.

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**20%**
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**40%**
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**60%**
ALTA	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5000 veces por año.	**80%**
MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	**100%**

Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

Para el cálculo de la probabilidad, se hace necesario resaltar que la frecuencia a la que se hace referencia para los riesgos de corrupción se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo. [9].

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

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

Determinación del impacto.

Para determinar el impacto de los riesgos de corrupción, se tiene en cuenta los siguientes criterios, de acuerdo con el cuadro **CRITERIOS PARA CALIFICAR EL IMPACTO -RIESGOS DE CORRUPCIÓN,** el cual permite establecer la zona de impacto de los riesgos de corrupción de acuerdo con las siguientes preguntas:

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

Catastrófico

Fuente: Adoptado de la Guía para la Administración de Riesgos y establecimientos de controles DAFP-2020 V.5

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	

Determinación del riesgo inherente y residual.

Para la determinación del riesgo inherente (antes de controles), se realiza de acuerdo a lo establecido para los riesgos de gestión, a través de la matriz de calor para establecer la calificación inicial del riesgo. Ver Numeral 8.2.2, del presente manual.

Zona de calificación riesgos de corrupción

MATRIZ CALIFICACIÓN DE RIESGOS					
Muy Alta 100%	ALTA	ALTA	ALTA	ALTA	EXTREMA
Alta 80%	MODERADA	MODERADA	ALTA	ALTA	EXTREMA
Media 60%	MODERADA	MODERADA	MODERADA	ALTA	EXTREMA
Baja 40%	BAJA	MODERADA	MODERADA	ALTA	EXTREMA
Muy Baja 20%	BAJA	BAJA	MODERADA	ALTA	EXTREMA
PROBABILIDAD	LEVE 20%	MENOR 40%	MODERADO 60%	MAYOR 80%	CATASTRÓFICO 100%
	IMPACTO				

8.6. 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.

8.6.1. Identificación de los activos de información.

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 presupuesta 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

8.6.2. 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:*

8.6.3. 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

8.6.4. 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 y 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-PS-DE-10 ART 2021

8.6.5. 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 **FM-PS-DE-10,** 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, lo cual obedece a la metodología para la valoración de los controles, acorde con la de los riesgos de gestión.

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. tIPO

Tipo de controles.

Los tipos de controles son los mismos que se han establecido para los riesgos de gestión corrupción, estos son:

Controles Preventivos: Son los que actúan en la entrada del proceso y antes de que se realice la actividad que origina el riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles detectivos: Son los que actúan durante la ejecución de la actividad. Detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen pueden generar costos implícitos.
De acuerdo con la forma como se ejecutan los controles, se clasifican en:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Se propenderá estructurar un Control que permita dar cobertura de carácter preventivo, detectivo y correctivo, los cuales deben tener las características de un control.

Los controles de Seguridad Digital tienen las mismas características de los riesgos de gestión y corrupción, conforme a la metodología establecida en el Numeral **8.3.1. Estructura de los Controles,** del presente Manual.

8.7. Mapas de Riesgos

El mapa de riesgo es el consolidado de los riesgos identificados en cada proceso, los riesgos residuales, planes de manejo y planes de contingencia. El mapa de cada proceso cuenta con el Formato **FM-PS-DE-09 Mapa de Riesgos** y del formato **FM-PS-DE-10 de Gestión de Riesgos de SD.**

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 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.

9. MONITOREO Y SEGUIMIENTO

9.1. 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.

9.2 Seguimiento a los mapas de riesgos.

La Oficina de Planeación, será quien apoye a la Entidad, en el seguimiento periódico a los planes de manejo de 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" [10].

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.

9.3. 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, el resultado del seguimiento que realice el Grupo de Control Interno, o los diferentes Entes de Control, se debe:

[10] 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 9.2** 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."

10. 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 llegarán a generar, dejando registro de estas.

11. 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