CAJA DE SUELDOS DE RETIRO
DE LA POLICÍA NACIONAL

PROCESO DE GESTIÓN INSTITUCIONAL

MANUAL DE ADMINISTRACIÓN DE RIESGOS

BOGOTA D.C.
2018

"CASUR HACIA LA INNOVACIÓN EN GESTIÓN Y SERVICIO"

GOBIERNO DE COLOMBIA

MINDEFENSA

Grupo Social y Empresarial de la Defensa
Por nuestras Fuerzas Armadas, para Colombia entera.

TABLA DE CONTENIDO

	Pág.
TABLA DE CONTENIDO	2
INTRODUCCION	5
OBJETIVO	6
TITULO 1. POLITICA DE ADMINISTRACION DEL RIESGO	6
ARTÍCULO 1. POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO.	6
ARTICULO 2. METODOLOGÍA	17
TITULO 2. DESARROLLO DE LA METODOLOGÍA	23
ARTÍCULO 3. ESTABLECIMIENTO DEL CONTEXTO DE LA ENTIDAD	23
ARTÍCULO 4. IDENTIFICACIÓN DEL RIESGO	25
ARTÍCULO 5. ANÁLISIS DEL RIESGO	26
ARTÍCULO 6. EVALUACIÓN DEL RIESGO	31
ARTÍCULO 7. MONITOREO Y REVISIÓN.	35
ARTÍCULO 8. REPORTE DE RIESGOS MATERIALIZADOS	38
ARTÍCULO 9. COMUNICACIÓN Y CONSULTA	39
TÍTULO 3. ALINEACION DEL MANUAL DE ADMINISTRACION DEL RIESGO	40
ARTÍCULO 10. POLÍTICAS DE LUCHA CONTRA LA CORRUPCIÓN Y DE EFICIENCIA ADMINISTRATIVA	40
ARTÍCULO 11. METODOLOGÍA PARA LOS RIESGOS DE CORRUPCIÓN	41

ARTÍCULO 12. METODOLOGÍA PARA LOS RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION 44

ARTÍCULO 13. METODOLOGIA PARA LA IDENTIFICACION DE LOS PELIGROS Y LA VALORACION DE LOS RIESGOS EN SEGURIDAD Y SALUD EN EL TRABAJO 68

ARTÍCULO 14. ALINEACIÓN CON EL MANUAL PARA LA IDENTIFICACIÓN Y COBERTURA DEL RIESGO EN LOS PROCESOS DE CONTRATACIÓN (AGENCIA NACIONAL PARA LA CONTRATACIÓN PÚBLICA) 78

ARTÍCULO 15. IDENTIFICACIÓN DE RIESGOS A LOS PROYECTOS 78

TÍTULO 4. MARCO LEGAL 78

Fecha	Descripción del Cambio	Responsable	Versión modificada
01/02/2016	Se ajusta la versión 5 del 21/10/2010, a la metodología de la Presidencia de la República, DAFP, y a la actualización del mapa de riesgos institucional	Oficina Asesora de Planeación	05
05/12/2016	Se ajusta la versión 6 del 01/02/2016, en los siguientes temas: tabla de nivel de impacto, costos de la posible afectación, definición del mapa de calor, indicadores de gestión del riesgo, metodología para riesgos de corrupción	Oficina Asesora de Planeación	06
12/12/2018	Se ajusta este documento en los siguientes temas: Introduccion, Artículo 1. Política para la Administración del Riesgo, Objetivos Específicos, Alcance, Términos y Definiciones, Articulo 2. Metodología, Modificacion de la Tabla 1. Responsabilidades frente a la administración del riesgo, Artículo 3. Establecimiento del contexto de la entidad, Modificacion de la Tabla 2. Contexto Interno, Externo y de Procesos, Artículo 4. Identificación del riesgo, Artículo 5. Análisis del riesgo, Artículo 6. Evaluación del riesgo, Artículo 7. Monitoreo y revisión, Artículo 12. Metodología para los Riesgos del Sistema de Gestión de Seguridad de la Información, Artículo 13, Metodología para la identificación de los peligros y la valoración de los riesgos en seguridad y salud en el trabajo, Artículo 14. Alineación con el manual para la identificación y cobertura del riesgo en los procesos de contratación (agencia nacional para la contratación pública) Artículo 15 Identificación de los riegos a los proyectos y Titulo 4 Marco Legal	Oficina Asesora de Planeación	07

Elaboró	Revisó	Aprobó
(ORIGINAL FIRMADO) **LILIANA GÓMEZ VÁSQUEZ** Técnico Oficina Planeación	**(ORIGINAL FIRMADO)** **DORA ILSA OSPINA OCAMPO** Jefe Oficina Planeación e informática	**(ORIGINAL FIRMADO)** **BG. (RA) JORGE ALIRIO BARÓN LEGUIZAMÓN** Director General

INTRODUCCION

La administración del riesgo ha tomado relevancia en la planeación y gestión de las entidades públicas, convirtiéndose ésta en una herramienta que permite dar respuesta a los cambios externos e internos que puedan generar incertidumbre en el cumplimiento de los objetivos propuestos. Es así que la consecuencia que genera dicha incertidumbre en la Entidad se denomina “Riesgo”.

Es importante recordar que el Estado Colombiano, mediante la ley 87 de 1993, establece que las entidades deben definir y aplicar las medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos, y su Decreto reglamentario 1537 de 2001, por el cual se establecen los elementos técnicos para el fortalecimiento de Sistema de Control Interno de las entidades de la Administración Pública, contempla la administración del riesgo como elemento probabilístico que permite aumentar la posibilidad del cumplimiento de objetivos.

Así mismo mediante Decreto 943 de 2014, por el cual se actualiza el Modelo Estándar de Control Interno (MECI), se establece como un componente del Módulo de Gestión y Control, la administración del riesgo que toma como insumo principal la planeación estratégica, la misión, visión, objetivos estratégicos, metas, entre otros; como herramienta de gestión y en cumplimiento del artículo 73 de la ley 1474 de 2011, las entidades deben contemplar mapa de riesgos de corrupción y las medidas concretas para mitigarlos, que se deben incluir en el mapa institucional que tenga la entidad.

De igual manera, mediante Decreto 1499 de 2017 se modificó el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 y define el Modelo Integrado de Planeación y Gestión MIPG estableciendo en uno de sus acápites los Comités Institucionales de Gestión y Desempeño encargado entre otras funciones de Adelantar y promover acciones permanentes de auto diagnóstico para facilitar la valoración interna de la gestión.

Por lo tanto la Caja de Sueldos de la Policía Nacional en virtud de cumplir las directrices establecidas por el Gobierno Nacional y con el objetivo de actualizar la administración del riesgo, establece como un proceso transversal la administración de riesgos a todas las actividades que se desarrollan al interior de la Entidad, para el cumplimiento de los objetivos estratégicos y de procesos. Es importante señalar que los responsables de realizar la administración de los riesgos, son los dueños de proceso con sus respectivos equipos de trabajo, para ello contarán con el acompañamiento y asesoría de la Oficina Asesora de Planeación y Control Interno, con fundamento en las metodologías que para el efecto determine el Departamento Administrativo de Función Pública DAFP y la Presidencia de la República.

OBJETIVO

El objetivo del presente documento es dar a conocer las políticas y la metodología, necesarias para establecer, implementar y mantener un sistema de administración de riesgos por proceso, acorde con la estructura y las necesidades de la Entidad, que permita la identificación, medición, control, monitoreo, así como el establecimiento de los planes de acción, indicadores de gestión y estrategias para el tratamiento de los riesgos identificados.

TITULO 1. POLITICA DE ADMINISTRACION DEL RIESGO

ARTÍCULO 1. POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO.

La Caja de Sueldos de Retiro de la Policía Nacional considera la administración del riesgo estratégica para el logro de la misión institucional y la toma de decisiones concernientes al Modelo Integrado de Planeación y Gestión y en tal virtud declara su compromiso con la adecuada identificación, valoración, mitigación y control de los riesgos que puedan afectar el cumplimiento de la ley, los objetivos estratégicos, los procesos de gestión, la satisfacción de los usuarios y el manejo transparente de los recursos públicos, mediante la definición de la metodología de administración del riesgo.

Del mismo modo, Casur declara su especial compromiso con el tratamiento del riesgo de corrupción y de aquellos identificados a partir de los aspectos e impactos ambientales, peligros (accidentes – incidentes) a la integridad de las personas, el medio ambiente, la seguridad de la información y la Seguridad y Salud en el Trabajo.

Conforme a la normatividad vigente Casur actualizará anualmente el mapa de riesgos institucional, con el fin de mitigarlos en el marco de la viabilidad jurídica, técnica, de recursos humanos, financieros y económicos dispuestos por la entidad; Los responsables de cada proceso, serán quienes adelanten la ejecución de los controles, las acciones preventivas y realicen el seguimiento a su cumplimiento como parte del autocontrol.

Objetivos Específicos

- Identificar los riesgos asociados a la implementación de un Sistema de Seguridad y Salud en el trabajo, al igual que la identificación y valoración de peligros (incidentes y/o accidentes) que puedan llegar a afectar la integridad física de los colaboradores en términos de “Lesión”, “enfermedad” o “muerte”.

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión de Seguridad de la Información, al igual que la identificación y valoración de “Activos de Información”.

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión Ambiental, al igual que la identificación y valoración de los “Aspectos e Impactos Ambientales”.

- Identificar los riesgos asociados a la implementación de un Sistema de Gestión de la Calidad, al igual que la identificación de los “procesos”, “procedimientos” y “actividades” críticas y/o complejas que no permitan alcanzar los objetivos institucionales.

- Identificar las causas y situaciones expresas asociadas al riesgo de corrupción, su valoración y tratamiento, a partir de la implementación de las directrices emitidas por la Secretaría de Transparencia de la Presidencia de la República, mediante el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.

ALCANCE

La administración de riesgo es de carácter estratégico en la Entidad, por lo tanto se aplicará a todos los procesos; lo cual contempla los riesgos asociados a la estrategia, la misionalidad, la operación; la gestión de los recursos y administración de los activos de Casur así como las acciones desplegadas por sus colaboradores durante el desarrollo de sus funciones y/o responsabilidades.

Niveles de Calificación del impacto

Los niveles para calificar el impacto fueron establecidos por la Dirección de la Caja de Sueldos de Retiro y su equipo directivo, teniendo como referencia los siguientes aspectos: la misión de Casur, recursos humanos, físicos, capacidad financiera y grupos sociales objetivo.

Niveles de aceptación del riesgo

Casur desarrollará la gestión del riesgo por procesos basada en los lineamientos emitidos por el DAFP, por lo cual se adopta la metodología de la siguiente manera: realizar la identificación del riesgo, realizar el análisis que permita, establecer los indicadores para calificar el impacto; Una vez determinada la zona de ubicación del riesgo, se realizará la evaluación de los controles existentes para cada uno y de esta manera, establecer el riesgo residual, al cual se le realizarán las acciones para su tratamiento. Como resultado de esta actividad se construirá el mapa de riesgos de la Entidad.

Términos y Definiciones:

Para el propósito del presente Manual, se aplican las siguientes definiciones:

TÉRMINOS RELATIVOS AL PLAN INICIAL DE IDENTIFICACIÓN / FASE DE IDENTIFICACIÓN.

Análisis de Contexto: Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y

objetivos de una institución. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político y legal, bien sea internacional, nacional o regional según sea el caso de análisis. Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta una entidad.

Análisis cuantitativo: el análisis cuantitativo utiliza valores numéricos para el impacto y la probabilidad.

Comité Institucional de Gestión y Desempeño: Comité para la Administración Integral de Riesgos.

Comunicación y consulta: Procesos continuos y reiterativos que CASUR lleva a cabo para suministrar, compartir u obtener información e involucrarse en un dialogo con las partes involucradas con respecto a la gestión del riesgo.

Descripción del Riesgo: Declaración estructurada del riesgo que usualmente contiene cuatro elementos: fuentes, eventos, causas y consecuencias. (GTC137:2011).

Dueño del proceso: Persona la cual tendrá asociada la responsabilidad del riesgo, diseñar y realizar control, seguimiento y monitoreo respectivo.

Escenario de Riesgo: es la representación de una situación en la cual una amenaza se materializa aprovechando una vulnerabilidad en un activo de información y causa un impacto visible para la Organización. Esto permite visualizar el nivel de impacto causado y la probabilidad de ocurrencia para poder realizar la calificación del riesgo.

Efecto: Desviación de aquello que se espera, sea positivo, negativo o ambos. Incertidumbre: Es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o posibilidad.

Fuente de un Riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (GTC137:2011). Puede ser tangible o intangible.

Fuentes de Riesgo: elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. Una fuente de riesgo puede ser tangible como por ejemplo lo asociado con la tecnología o a las instalaciones y lo intangible como por ejemplo la situación sociocultural, entorno económico, clima político y entorno familiar. [Fuente: ISO 31000].

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: consecuencias que puede causar a la compañía la ocurrencia del riesgo.

Mapa de Riesgo Institucional: Herramienta que permite realizar un inventario de los riesgos

residuales de la Entidad.
Matriz de riesgos: Documento formal donde se registra los riesgos de seguridad de la información vigentes para la Entidad con base en el formato definido en la metodología.

Mitigación (reducción): planificación y ejecución de medidas de intervención, dirigidas a reducir o disminuir el riesgo.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa que permite verificar cambios con respecto al nivel de desempeño exigido o esperado.

Parte Interesada: persona u organización que puede afectar, verse afectada o percibirse así misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada. [Fuente: ISO 31000].

Partes Interesadas: Persona o grupo dentro o fuera del lugar de trabajo (véase el numeral 2.18) involucrado o afectado por el desempeño de seguridad y salud ocupacional de una organización (NTC-OHSAS 18001).

Propietario del Riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (GTC137:2011).

Riesgo: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. (Guía de Admón. De Riesgos DAFP Septiembre 2011).

Riesgo: Algo que podría suceder y afectar el logro de los objetivos organizacionales. (GTC 176)

Riesgo: Efecto de la incertidumbre sobre los objetivos. (GTC137: 2011)

Riesgo: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) [Fuente: ISO 31000].

Riesgo: Combinación de la probabilidad de que ocurra(n) un(os) evento(s) o exposición(es) peligroso(s), y la severidad de lesión o enfermedad, que puede ser causado por el (los) evento(s) o la(s) exposición(es) (NTC-OHSAS 18001

Riesgos Transversales: Eventos que aunque tienen como propietario a un solo proceso, pueden ser causa o efecto de otros eventos de riesgo para los demás procesos de la entidad:

Nota 1: Generalmente los procesos propietarios de los riesgos transversales son los de Soporte.

TÉRMINOS RELATIVOS A LA FASE DEFINICIÓN DE LA GESTIÓN

Alcance de un Proyecto: Trabajo que debe realizarse para entregar un producto, servicio o resultado con las características y funciones especificadas (PMBOK, 4ta. Edición).

Control: Medida o acción que modifica el riesgo mediante la afectación ya sea de la probabilidad o del impacto. (GTC137:2011).

Consecuencia: Resultado de un evento que afecta a los objetivos. (GTC137:2011)

Consecuencia: Resultado, en términos de lesión o enfermedad, de la materialización de un riesgo, expresado cualitativa o cuantitativamente

Consecuencias: Resultado del evento que puede ser cierto o incierto y tener efectos positivos o negativos para la entidad y que puede expresarse en términos cualitativos o cuantitativos. Una consecuencia inicial puede tener mayor impacto considerando los efectos secundarios. [Fuente: ISO 31000].

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo (probabilidad e impacto antes de controles), con los criterios del riesgo (valoración de controles) para determinar si el riesgo, su magnitud o ambos, son aceptables o tolerables. (GTC137:2011)

Exposición: Extensión hasta la cual una organización, una parte involucrada o ambas están sujetas a un evento. (GTC137:2011).

Exposición: Situación en la cual las personas se encuentran en contacto con los peligros.

Frecuencia: Número de eventos o efectos por unidad de tiempo definida. (GTC137:2011)

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo. (GTC137: 2011).

Identificación del riesgo: Fase en la cual se realiza la identificación de los riesgos, basados en la estructura y contexto definido, puede hacerse a cualquier nivel desde el estratégico hasta el operativo.

Matriz de Valoración de Riesgos: Herramienta para la evaluación de los riesgos y su clasificación. También se le dice matriz RAM por sus siglas en ingles. (Matriz Risk Assessment Matrix). La matriz permite calificar y evaluar los riesgos en términos de impacto y probabilidad.

Nivel de Riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad. Sumatoria de la multiplicación de la probabilidad por el impacto de todos los riesgos de un proceso o de la Institución. (GTC137:2011).

Nivel de riesgo: Magnitud de un riesgo (véase el numeral 2.31 (GTC-45).) resultante del producto del nivel de probabilidad (véase el numeral 2.24) por el nivel de consecuencia (véase el numeral 2.21 (GTC-45).).

Probabilidad: Oportunidad de que algo suceda. (Likehood). (GTC137:2011).

Probabilidad: Grado de posibilidad de que ocurra un evento no deseado y pueda producir consecuencias (véase el numeral 2.5 (GTC-45).).

Probabilidad: Posibilidad de que algo ocurra bien sea que se haya definido, medido, o estimado objetiva o subjetivamente, o en términos de los descriptores generales (tales como raro, improbable, probable, casi cierto). La probabilidad puede expresarse cuantitativa o cualitativamente).

Proyecto: Es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

Proyecto: Proceso único consistente en un conjunto de actividades coordinadas y controladas con fechas de inicio y de finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos, incluyendo las limitaciones de tiempo, costo y recursos. (ISO9000:2005)

Nota 1: Un proyecto individual puede formar parte de la estructura de un proyecto mayor.

Nota 2: En algunos proyectos, los objetivos se afinan y las características del producto se definen progresivamente según evolucione el proyecto.

Nota 3: El resultado de un proyecto puede ser una o varias unidades de producto (3.4.2).

Programa: Un programa es una unidad lógica organizada y coherente de actividades orientada a un propósito superior.

Plan: Los planes son instrumentos de operacionalización macro, mediante los cuales la Institución ordena y organiza programas, proyectos. Por su naturaleza temporal, tienen un principio y un final definidos. (PMBOK, 4ta. Edición).

Riesgo Residual: Remanente después del Tratamiento del Riesgo. (GTC137:2011). Es aquel que permanece aún después de desarrolladas las acciones de tratamiento del riesgo. Capacidad total de riesgo que una organización está dispuesta a aceptar, tolerar o asumir en cualquier momento dado.

Tratamiento del Riesgo: Proceso para modificar el riesgo (GTC137:2011). Conjunto de acciones que permiten a través de la creación, fortalecimiento o implementación de controles, modificar la probabilidad o el impacto de un riesgo. (Un plan de tratamiento del riesgo, puede derivar o constituirse en un proyecto y/o programa de acuerdo al tema a mitigar o mejorar).

TÉRMINOS RELATIVOS A LA FASE GESTIÓN DE RIESGOS

Acción Correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable. (ISO9000:2005).

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. (ISO9000:2005).

Autoridad: Poder con que se cuenta o que se ha recibido por delegación. (NTCGP1000:2009).

Corrección: Acción tomada para eliminar una no conformidad detectada. (ISO9000:2005).

Evento: Ocurrencia o cambio de un conjunto partículas de circunstancias. (GTC137:2011) en algunas ocasiones se hace referencia a un evento como un “incidente” o “accidente”.

Eventos: presencia o cambio de un conjunto particular de circunstancias, que puede ser una o varias ocurrencias con una o varias causas. Un evento puede consistir en algo que no está sucediendo. [Fuente: ISO 31000].

Eventos Potenciales a Evaluar: Son aquellas situaciones ocurridas en un proceso que podrían llegar a ser clasificadas como riesgos materializados, pero se debe hacer un análisis previo para llegar a esa conclusión.

Plan de Contingencia: Las acciones o planes de contingencia garantizan que la Institución tiene la capacidad de seguir prestando sus servicios sin interrupciones o con periodos mínimos de interrupción, ante eventos inesperados como terremotos, fallas de sistemas de información, cortes del suministro de servicios públicos, inundaciones, terrorismo, atentados a funcionarios y/o instalaciones, entre otros. Deben estar previamente elaborados, socializados y aprobados para su ejecución. Estos no cuentan con un procedimiento, formato o guía para su elaboración.

Queja: Es la manifestación verbal o escrita de protesta, censura, descontento e inconformidad que eleva un ciudadano ante la insatisfacción que le causa la prestación del servicio de uno o varios de sus funcionarios.

Reclamo: Es el derecho que tiene toda persona de exigir, reivindicar o demandar una solución o respuesta relacionada con la prestación indebida de un servicio.

Registro: Tipo de documento que da evidencia del cumplimiento de un requisito o de la realización de una actividad. Ejemplo: acta de reunión, informe de auditoría, etc.

Revisión por la Dirección: Revisión sistemática y planificada que hace la Alta Dirección del estado general del sistema, con el fin de tomar decisiones que propicien su mejora continua.

Riesgo Materializado: Ocurrencia de un evento que se había identificado como incierto.

Satisfacción del Cliente: Percepción que el cliente tiene sobre el grado en que se han cumplido sus requisitos. (ISO 9000:2005).

Sugerencia: Es la opinión o insinuación que eleva una persona para adecuar o mejorar un proceso o la prestación de un servicio.

TÉRMINOS RELATIVOS A LA FASE MEDICIÓN DE LA GESTIÓN

Causa Raíz: Es el origen de una falla o incumplimiento.

Control: Medida o acción que modifica el riesgo mediante la afectación ya sea de la probabilidad o del impacto. (GTC137:2011).

Control: Medio para mantener el riesgo en un nivel aceptable. Los controles pueden ser administrativos, técnicos o legales y pueden materializarse en políticas, procedimientos, guías, lineamientos, prácticas y estructuras organizacionales.

Plan de Tratamiento: Conjunto de acciones que se planean y se ejecutan con el fin de generar controles que eviten la materialización de un riesgo o disminuyan su impacto en caso de que ocurra. (GTC137:2011).

Términos relativos a la fase de cierre

Aciertos: Experiencias exitosas, aspectos que pueden ser replicables, fortalezas, logros, cumplimiento de los objetivos trazados en términos institucionales

Desaciertos: Acciones / planes que no arrojaron los resultados esperados, deficiencias en la planeación, fracasos.

Lección Aprendida: Conocimiento adquirido a través de la experiencia organizacional, que analizado y difundido apropiadamente puede convertirse en acciones que lleven a la Institución a obtener mejores resultados, no repitiendo las acciones erróneas y replicando las que condujeron al éxito, considerando en todo momento un contexto de seguridad en constante transformación.

TÉRMINOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN.

Aceptación del riesgo: La decisión informada para tomar un riesgo en particular. [Fuente: ISO27000].

Activo: Es todo aquello que posea valor para la entidad. Ejemplo: información en formato físico y/o digital; el software; el hardware; los servicios de información, de comunicaciones, de almacenamiento, etc.; las personas y otros.

Administración de riesgos: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

Amenaza: causa potencial de in incidente no deseado, el cual puede resultar en daño al

sistema o a la Organización. [Fuente: ISO 27000].
Ataque: Intento de destruir, exponer, deshabilitar, alterar, o lograr acceso no autorizado o de hacer un uso no autorizado de un activo.

Confidencialidad: propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos. [Fuente: ISO 27000].

Control de Acceso: Medios para asegurar que el acceso a los activos es autorizado y restringido de acuerdo a los requerimientos del negocio y de la seguridad.

Custodio: Es una parte designada de Policía Nacional la cual puede ser un cargo, un proceso o un grupo de trabajo, quien se encuentra encargado de administrar y hacer efectivos los controles de seguridad que el propietario del activo haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Diagnóstico: Análisis del estado actual de cumplimiento que tiene una entidad, con respecto a los objetivos de control basados en la norma ISO 27001:2013 y adaptados por Min TIC a las necesidades del entorno colombiano.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada. [Fuente: ISO 27000].

Información: Datos relacionados que tienen significado para la Policía Nacional. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Información documentada: Información que requiere ser controlada y mantenida por una organización y el medio en el cual está contenida.

Integridad: Propiedad que permite salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento.

Seguridad de la Información: La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio.

Causas: Debilidad de un activo o control, que puede ser explotada por una o más amenazas.

Vulnerabilidad: debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información

TÉRMINOS RELATIVOS A LA SEGURIDAD Y SALUD EN EL TRABAJO (GTC -45)

Accidente de trabajo. Suceso repentino que sobreviene por causa o con ocasión del trabajo, y que produce en el trabajador una lesión orgánica, una perturbación funcional, una invalidez o la

muerte. Es también accidente de trabajo aquel que se produce durante la ejecución de órdenes del empleador o durante la ejecución de una labor bajo su autoridad, incluso fuera del lugar y horas de trabajo (Decisión 584 de la Comunidad Andina de Naciones).

Actividad rutinaria: Actividad que forma parte de un proceso de la organización, se ha planificado y es estandarizable.

Actividad no rutinaria: Actividad que no se ha planificado ni estandarizado, dentro de un proceso de la organización o actividad que la organización determine como no rutinaria por su baja frecuencia de ejecución.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo (véase el numeral 2.31 (GTC-45).) y para determinar el nivel del riesgo (véase el numeral 2.25 (GTC-45).) (ISO 31000).

Competencia: Atributos personales y aptitud demostrada para aplicar conocimientos y habilidades.

Diagnóstico de condiciones de trabajo: Resultado del procedimiento sistemático para identificar, localizar y valorar "aquellos elementos, peligros o factores que tienen influencia significativa en la generación de riesgos para la seguridad y la salud de los trabajadores. Quedan específicamente incluidos en esta definición:

a) Las características generales de los locales, instalaciones, equipos, productos y demás útiles existentes en el lugar de trabajo;
b) La naturaleza de los peligros físicos, químicos y biológicos presentes en el ambiente de trabajo, y sus correspondientes intensidades, concentraciones o niveles de presencia;
c) Los procedimientos para la utilización de los peligros citados en el apartado anterior, que influyan en la generación de riesgos para los trabajadores; y
d) La organización y ordenamiento de las labores incluidos los factores ergonómicos y psicosociales" (Decisión 584 de la Comunidad Andina de Naciones).

Diagnóstico de condiciones de salud: Resultado del procedimiento sistemático para determinar "el conjunto de variables objetivas de orden fisiológico, psicológico y sociocultural que determinan el perfil sociodemográfico y de morbilidad de la población trabajadora" (Decisión 584 de la Comunidad Andina de Naciones).

Elemento de Protección Personal (EPP): Dispositivo que sirve como barrera entre un peligro y alguna parte del cuerpo de una persona.

Enfermedad: Condición física o mental adversa identificable, que surge, empeora o ambas, a causa de una actividad laboral, una situación relacionada con el trabajo o ambas (NTC-OHSAS 18001).

Enfermedad profesional: Todo estado patológico que sobreviene como consecuencia obligada de la clase de trabajo que desempeña el trabajador o del medio en que se ha visto obligado a trabajar, bien sea determinado por agentes físicos, químicos o biológicos (Ministerio

de la Protección Social, Decreto 2566 de 2009).
Equipo de protección personal: Dispositivo que sirve como medio de protección ante un peligro y que para su funcionamiento requiere de la interacción con otros elementos.

Evaluación higiénica: Medición de los peligros ambientales presentes en el lugar de trabajo para determinar la exposición ocupacional y riesgo para la salud, en comparación con los valores fijados por la autoridad competente.

Evaluación del riesgo: Proceso para determinar el nivel de riesgo (véase el numeral 2.25) asociado al nivel de probabilidad (véase el numeral 2.24 (GTC-45).) y el nivel de consecuencia (véase el numeral 2.21 (GTC-45).).

Identificación del peligro: Proceso para reconocer si existe un peligro (véase el numeral 2.27 (GTC-45).) y definir sus características.

Incidente: Evento(s) relacionado(s) con el trabajo, en el (los) que ocurrió o pudo haber ocurrido lesión o enfermedad (independiente de su severidad) o víctima mortal (NTC-OHSAS 18001).

Nota 1: Un accidente es un incidente que da lugar a una lesión, enfermedad o víctima mortal.

Nota 2: Un incidente en el que no hay como resultado una lesión, enfermedad ni víctima mortal también se puede denominar como “casi-accidente” (situación en la que casi ocurre un accidente).

Nota 3: Una situación de emergencia es un tipo particular de accidente.

Nota 4: Para efectos legales de investigación, tener en cuenta la definición de incidente de la resolución 1401 de 2007 del Ministerio de la Protección Social o aquella que la modifique, complemente o sustituya.

Lugar de trabajo: Espacio físico en el que se realizan actividades relacionadas con el trabajo, bajo el control de la organización (NTC-OHSAS 18001).

Medida(s) de control: Medida(s) implementada(s) con el fin de minimizar la ocurrencia de incidentes.

Monitoreo biológico: Evaluación periódica de muestras biológicas (ejemplo sangre, orina, heces, cabellos, leche materna, entre otros) tomadas a los trabajadores, con el fin de hacer seguimiento a la exposición a sustancias químicas, a sus metabolitos o a los efectos que éstas producen en los trabajadores.

Nivel de consecuencia (NC): Medida de la severidad de las consecuencias (véase el numeral 2.5 (GTC-45).).

Nivel de deficiencia (ND): Magnitud de la relación esperable entre (1) el conjunto de peligros detectados y su relación causal directa con posibles incidentes y (2), con la eficacia de las

medidas preventivas existentes en un lugar de trabajo.
Nivel de exposición (NE): Situación de exposición a un peligro que se presenta en un tiempo determinado durante la jornada laboral.

Nivel de probabilidad (NP): Producto del nivel de deficiencia (véase el numeral 2.22 (GTC-45).) por el nivel de exposición (véase el numeral 2.23 (GTC-45).).

Peligro: Fuente, situación o acto con potencial de daño en términos de enfermedad o lesión a las personas, o una combinación de éstos (NTC-OHSAS 18001).

Personal expuesto: Número de personas que están en contacto con peligros.

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados (NTC-ISO 9000).

Riesgo aceptable: Riesgo que ha sido reducido a un nivel que la organización puede tolerar, respecto a sus obligaciones legales y su propia política en seguridad y salud ocupacional (NTC-OHSAS 18001).

Valoración de los riesgos: Proceso de evaluar el(los) riesgo(s) que surge(n) de un(os) peligro(s), teniendo en cuenta la suficiencia de los controles existentes y de decidir si el(los) riesgo(s) es (son) aceptable(s) o no (NTC-OHSAS 18001).

Valores límite permisible (VLP): son valores definidos por la American Conference of Governmental Industrial Hygienists (ACGIH). El VLP se define como la concentración de un contaminante químico en el aire, por debajo del cual se espera que la mayoría de los trabajadores puedan estar expuestos repetidamente, día tras día, sin sufrir efectos adversos a la salud. En Colombia, los niveles máximos permisibles se fijan de acuerdo con la tabla de Threshold Limit Values (TLV), establecida por la American Conference of Governmental Industrial Hygienists (ACGIH), a menos que sean fijados por alguna autoridad nacional competente (Resolución 2400 de 1979 del Ministerio del Trabajo y Seguridad Social, art. 154).

ARTICULO 2. METODOLOGÍA

La gestión del riesgo se fundamenta en el desarrollo de las etapas que se presentan a continuación:

Gráfica 1. Metodología de administración del riesgo

El proceso de administración de riesgos debe propender por la creación de una cultura institucional activa, constante y persistente en el manejo de los riesgos, en el seguimiento y monitoreo de los riesgos existentes, apoyando a los responsables en la creación de tratamientos efectivos que faciliten la consecución de los objetivos propuestos para la continuidad y desarrollo de la Institución.

Clasificación del riesgo

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad, su Manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

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

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de

excedentes de tesorería y el manejo sobre los bienes.

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

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

Riesgos de Corrupción: Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

Periodicidad de monitoreo y seguimiento

En el ejercicio de autoevaluación trimestral, realizada por cada dueño de proceso, se deberán monitorear y revisar los riesgos mediante el formato PGP-FR- 04 METODOLOGIA AUTOEVALUACION DE LA GESTION Y EL CONTROL, sin que esto afecte la actividad de seguimiento que realice la Oficina de Control Interno.

En cuanto a la periodicidad del seguimiento, para los riesgos asociados a posibles actos de corrupción, se debe dar cumplimiento a las fechas establecidas por la guía de la Secretaría de transparencia, denominada “Guía para la gestión del riesgo de corrupción 2015. Las frecuencias de medición serán de manera cuatrimestral, de forma que permitan que el seguimiento realizado sea base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

Niveles de responsabilidad frente al riesgo

La responsabilidad por el cumplimiento y la aplicación de esta política recae en los subdirectores, coordinadores, jefes de oficina y en general, los servidores públicos y contratistas de la Entidad. Es compromiso de todos los servidores públicos y de la Alta Dirección, velar por el control de todos los riesgos que afecten al cumplimiento de los objetivos de CASUR y para ello, deben establecer controles eficientes, seguimientos y monitoreo necesarios que aseguren el cumplimiento de las metas y la continuidad del servicio.

CARGO/AREA	RESPONSABILIDAD
Línea Estratégica -	• Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad • Establecer la Política de Administración del Riesgo • Asumir la responsabilidad primaria del SCI y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo • Específicamente el Comité Institucional de Coordinación de Control Interno, evaluar y dar línea sobre la administración de

Alta dirección , Comité Institucional de Coordinación de Control Interno, Comité Institucional de Gestión y Desempeño, Oficial de Seguridad de la Información	los riesgos en la entidad • Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. • Así mismo, hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles • Establecer las políticas de operación encaminadas a controlar los riesgos que pueden llegar a incidir en el cumplimiento de los objetivos institucionales • Hacer seguimiento a la adopción, implementación y aplicación de controles • Será el responsable de hacer cumplir la política de Administración del Riesgo establecida en el presente manual. • Establece los lineamientos para la administración integral de los riesgos de CASUR. • Es el responsable por el análisis de riesgos de seguridad de la información en concurso con los dueños de proceso quienes desarrollaran la metodología para sus levantamiento • Actuar oportunamente ante las alertas para llevar a cabo el análisis de riesgos.
Primera Línea – Líderes de proceso Primera Línea – Líderes de proceso	• Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales • Definen y diseñan los controles a los riesgos • A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecen los mapas de riesgos • Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad • Mantener controles internos efectivos para ejecutar procedimientos de riesgo y control en el día a día • Diseñar e implementar procedimientos detallados que sirvan como controles, a través de una estructura de responsabilidad en cascada, y supervisar la ejecución de esos procedimientos por parte de los servidores públicos a su cargo • Establecer responsabilidades por las actividades de control y asegurar que personas competentes, con autoridad suficiente, efectúen dichas actividades con diligencia y de manera oportuna • Asegurar que el personal responsable investigue y actúe sobre

	asuntos identificados como resultado de la ejecución de actividades de control • Diseñar e implementar las respectivas actividades de control. Esto incluye reajustar y comunicar políticas y procedimientos relacionados con la tecnología y asegurar que los controles de TI son adecuados para apoyar el logro de los objetivos • Elaborar y actualizar el mapa de riesgos institucional (riesgos de gestión y riesgos de corrupción del proceso), cada vez que surjan cambios al interior de la Entidad, o siempre y cuando la normatividad lo exija y al inicio de cada vigencia • Velar por el cumplimiento de los planes de acción e indicadores de gestión del mapa de riesgos. • Socializar el mapa de riesgos con las diferentes dependencias involucradas en los riesgos. • Verificar la ejecución adecuada de los controles de mitigación de los riesgos • Realizar monitoreo y seguimiento a los riesgos en la evaluación trimestral • Elaborar y documentar las acciones adelantadas cuando el riesgo se materialicen
Segunda Línea – Servidores responsables de monitoreo y evaluación de controles y gestión del riesgo	• Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada • Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude • Ayudar a la primera línea con evaluaciones del impacto de los cambios en el SCI • Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento • Consolidar los seguimientos a los mapas de riesgo • Establecer un líder de la gestión de riesgos para coordinar las actividades en esta materia • Elaborar informes consolidados para las diversas partes interesadas • Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar • Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas • Supervisar el cumplimiento de las políticas y procedimientos específicos establecidos por la primera línea de defensa • Asistir a la gerencia operativa en el desarrollo y comunicación de políticas y procedimientos • Asegurar que los riesgos son monitoreados en relación con la política de administración de riesgo establecida para la entidad

Oficina Asesora de Planeación	• Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser Necesario • Supervisar el cumplimiento de las políticas y procedimientos específicos establecidos por la primera línea • Realizar monitoreo de los riesgos y controles tecnológicos • Grupos como los departamentos de seguridad de la información también pueden desempeñar papeles importantes en la selección, desarrollo y mantenimiento de controles sobre la tecnología, según lo designado por la administración • Establecer procesos para monitorear y evaluar el desarrollo de exposiciones al riesgo relacionadas con tecnología nueva y emergente • Consolidación del mapa de riesgos institucional. • Publicación del mapa de riesgos institucional en la herramienta Suite Visión Empresarial • Realizar monitoreo y seguimiento a los riesgos en la evaluación trimestral. • Brindar acompañamiento y asesoría a los procesos para el manejo del módulo gestión del riesgo. • Revisar y/o ajustar el mapa institucional donde estarán incluidos los riesgos de corrupción, lo cual implica que los dueños de proceso deberán efectuar trimestralmente el monitoreo, con el fin de identificar los cambios y tomar las acciones correspondientes.
Tercera Línea – Oficina de Control Interno Tercera Línea – Oficina de Control	• Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa • Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna • Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías • Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad • Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas • Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos • Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles. • Proporcionar seguridad razonable con respecto al diseño e

Interno	implementación de políticas, procedimientos y otros controles • Evaluar si los procesos de gobierno de TI de la entidad apoyan las estrategias y los objetivos de la entidad • Proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos y, según sea apropiado, puede recomendar mejoras a las actividades de control específicas • Realizar el seguimiento a los riesgos que a nivel institucional han sido consolidados. En sus procesos de auditoría interna dicha oficina debe analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos, haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles. • Realiza el seguimiento a los riesgos de corrupción en los tiempos establecidos en la guía para la gestión del riesgo de corrupción 2015

Tabla 1. Responsabilidades frente a la administración del riesgo

TITULO 2. DESARROLLO DE LA METODOLOGÍA

ARTÍCULO 3. ESTABLECIMIENTO DEL CONTEXTO DE LA ENTIDAD

El establecimiento del contexto hace referencia a la definición de los parámetros internos, externos y de procesos que se han de tomar en consideración para la administración del riesgo de la Entidad. El establecimiento del contexto se debe realizar previamente de la identificación de los riesgos, teniendo en cuenta la Misión, Visión y Objetivos Estratégicos de la Entidad. Para esto se llevan a cabo mesas de trabajo con los líderes de los procesos y su equipo de trabajo con quienes se identifican Debilidades, Oportunidades, Fortalezas y Amenazas, que puedan generar riesgos que impacten el logro de los objetivos institucionales (Riesgos Estratégicos) y el logro de los objetivos del proceso (Riesgos Operativos).

Para el establecimiento del contexto es necesario que los participantes en las mesas de trabajo, estandaricen su percepción y conocimiento acerca de los lineamientos estratégicos y procedimentales que guían a la Entidad. Para la definición del contexto externo, se verifican aspectos tales como:

Ambiente de negocio, social, reglamentario, cultural, competitivo, financiero y político, políticas económicas, sociales y tecnológicas.

- Las partes externas involucradas.
- Es particularmente importante considerar las concepciones y los valores de las partes externas involucradas y establecer políticas para la comunicación de esas partes.

- Las condiciones del país y las diferentes ciudades en donde tiene participación la Entidad.

Para la definición del contexto interno, se verifican aspectos tales como:

- Cultura organizacional.
- Partes internas involucradas, funciones y responsabilidades.
- Estructura Organizacional.
- Capacidades en términos de recursos tales como personas, sistemas, procesos, tecnología y capital.
- Políticas, Objetivos y Estrategias implementadas.
- Análisis de las PQRS

Para la definición del contexto de procesos, se verifican aspectos tales como:

- Identificación dentro de la cadena de valor
- Sinergia e Interacción de los procesos,
- Cumplimiento de los objetivos en su operación
- Cliente (interno-externo) y sus partes interesadas

A continuación se describe una síntesis del contexto actual de la Caja de Sueldos de Retiro, así:

CONTEXTO INTERNO	CONTEXTO EXTERNO	CONTEXTO PROCESOS
• Ausencia de un sistema de información integral e integrado sobre necesidades y expectativas del afiliado • Deficiencia en mecanismos para consultar y escuchar la voz del afiliado. • Insuficiente planta de personal. • Resistencia al cambio de la población afiliada hacia los procesos de transformación. • Escasas alternativas de financiación para incrementar recursos propios.	• Alta litigiosidad generada por la normatividad en materia prestacional. • Incremento en el período de vida de las asignaciones de retiro. • El estado percibe a CASUR, como un gasto administrativo. • Creciente impacto económico de las asignaciones de retiro en el gasto público por incremento de la planta en la Policía Nacional. • Implementación de la Cuenta Única Nacional. • Propuestas de eliminación de los regímenes especiales.	• Desactualización normativa de algunos de los proceso y procedimientos • Falta de articulación en los procesos. • Debilidad en control y medición de la Gestión. • Debilidad en la documentación de las políticas de seguridad de la información • Debilidad en la documentación de las acciones de mejora • Deficiencias en el proceso de liquidación de las sentencias.

CONTEXTO INTERNO	CONTEXTO EXTERNO	CONTEXTO PROCESOS
• Experiencia de la entidad en proceso de reconocimiento y pago • Satisfacción y confiabilidad de los afiliados en el pago de sus asignaciones con recursos propios • Participación gradual de la entidad en el pago de las asignaciones con recursos propios. • Nuevo direccionamiento estratégico hacia la reformulación del rumbo institucional. • Efectividad en modelo de administración de propiedades e infraestructura física. • Mantenimiento y sostenibilidad de la infraestructura física y tecnológica. • Profesionalización y fortalecimiento de la planta de cargos	• Proyecto de creación del Ministerio de Seguridad Ciudadana. • Población cautiva con tendencia creciente. • Desarrollo del modelo de aprovechamiento de la estructura física • Ley 923 de 2004, fondo especial para la construcción de reservas. • Respaldo sectorial a proyectos para optimizar y mejorar el sistema de información al usuario. • Demanda creciente de arrendamientos de propiedades de alta valoración. • Desarrollo de las Tics como política gubernamental. • Índice de satisfacción positivo de la población filiada. • Adopción de normas internacionales de contabilidad en Colombia • Implementación del modelo integrado de planeación y gestión • Implementación de las políticas de seguridad de la información	• Implementación de los sistemas de gestión de calidad, sistema de gestión ambiental y sistema de gestión de seguridad y salud en el trabajo. • Debilidad en control y medición de la Gestión

Tabla 2. Contexto Interno, Externo y de Procesos

ARTÍCULO 4. IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo se realizará determinando las causas, con base en el contexto interno, externo definido, teniendo en cuenta aquellos que pueden afectar el logro de los objetivos institucionales y de proceso. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis de contexto correspondiente, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este levantamiento de causas se procederá a identificar el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden afectar el normal desarrollo de los objetivos del proceso; es necesario referirse a sus características o las formas en que se observa o manifiesta.

Para la realización de esta etapa se establece la siguiente estructura:

IDENTIFICACIÓN DE RIESGOS						
N° Riesgo	Riesgo	Tipo de Riesgo	Causa Raíz	Causas	Consecuencia /Efecto	Imperativo Afectado

Tabla 3. Matriz de Identificación de Riesgos

Para la identificación de los riesgos se diligencia la matriz con la siguiente información:

N° Riesgo: Código del riesgo determinado por la Entidad.

Riesgo: Enuncie el riesgo identificado.

Tipo de Riesgo: Se refiere a la clasificación del riesgo dada en el artículo 1 2 del Título 2 1 del presente documento.

Causa Raíz: Es la causa principal que aumenta la probabilidad de ocurrencia del riesgo identificado; se identifica mediante la utilización de alguna de las metodologías establecidas en la guía de mejora de la entidad.

Causas: Se enuncian las demás circunstancias generadores del Riesgo.

Consecuencias / Efectos: Enuncie las consecuencias ante la posible materialización del riesgo. Se expresan en términos de Daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen de credibilidad, de confianza, interrupción del servicio y daño ambiental.

Imperativo afectado: En esta casilla se relaciona imperativo y el objetivo de la planeación estratégica que se afecta ante la ocurrencia del evento desfavorable.

ARTÍCULO 5. ANÁLISIS DEL RIESGO

Establece 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). Para su medición se tendrá en cuenta lo siguiente:

Probabilidad de Ocurrencia: para su determinación se utiliza la tabla de probabilidad, esta puede ser medida bajo los criterios de frecuencia o factibilidad. La frecuencia, analiza el número de eventos en un periodo determinado; se trata de hechos que se han materializado o

se cuenta con un historial de situaciones o de eventos asociados al riesgo y la factibilidad analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que se dé.
En caso de no contar con datos históricos, bajo el concepto de factibilidad se trabajará de acuerdo con la experiencia de los funcionarios que desarrollan el proceso y de sus factores internos y externos. Para determinar el valor de la probabilidad se establecen los siguientes niveles:

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

Tabla 4. Escalas de probabilidad

Consecuencia o nivel de impacto: Bajo el criterio de Impacto, el riesgo se debe medir a partir de las siguientes especificaciones, contenidas en la tabla de impactos o consecuencias, la cual fue establecida por la alta Dirección de la Caja de Sueldos de Retiro y su equipo directivo de acuerdo a la metodología del DAFP, siendo concertada en la política de riesgos institucionales:

Para su determinación se utilizan las siguientes tablas de niveles de impacto:

ESCALAS CUALITATIVAS:

NIVELES	CUALITATIVO
5. Catastrófico	• Interrupción de las operaciones de la Entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Perdida de información crítica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

NIVELES	CUALITATIVO
4. Mayor	• Interrupción de las operaciones de la Entidad entre 2 y 5 días. • Pérdida de información crítica que pueda ser recuperada de forma parcial o incompleta. • sanción por parte del ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. • Imagen institucional afectada en el orden nacional o regional
3. Moderado	• Interrupción de las operaciones de la Entidad por 1 día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. • Imagen institucional afectada en el orden nacional o regional por retrasos en la operación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias.
2. Menor	• Interrupción de las operaciones de la Entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
1. Insignificante	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.

Tabla 5. Escalas de Impacto cualitativa

ESCALAS CUANTITATIVAS:

NIVELES	CUANTITATIVO
5. Catastrófico	• Impacto que afecte el valor presupuestal en un valor >7.201 SMLMV • Pérdida de cobertura en la prestación de los servicios de le entidad >50%. • Pago de indemnizaciones a terceros por acciones legales que pueden llegar a afectar el presupuesto total de la entidad en un valor >7.201 SMLMV • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor >7.201 SMLMV

NIVELES	CUANTITATIVO
4. Mayor	• Impacto que afecte el presupuesto, en un valor entre 5.501 SMLMV y 7.200 SMLMV. • Pérdida de cobertura en la prestación de los servicios de le entidad entre un 21% y 50 %. • Pago de indemnizaciones a terceros por acciones legales que pueden llegar a afectar el presupuesto total de la entidad en un valor entre 5.501 SMLMV y 7.200 SMLMV. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor entre 5.501 SMLMV y 7.200 SMLMV.
3. Moderado	• Impacto que afecte el presupuesto, en un valor entre 3.001 SMLMV y 5.500 SMLMV • Pérdida de cobertura en la prestación de los servicios de le entidad entre 11 y 20%. • Pago de indemnizaciones a terceros por acciones legales que pueden llegar a afectar el presupuesto total de la entidad en un valor entre 3.001 SMLMV y 5.500 SMLMV • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor entre 3.001 SMLMV y 5.500 SMLMV
2. Menor	• Impacto que afecte el presupuesto, en un valor entre 701 SMLMV y 3.000 SMLMV. • Pérdida de cobertura en la prestación de los servicios de le entidad entre 5 y 10%. • Pago de indemnizaciones a terceros por acciones legales que pueden llegar a afectar el presupuesto total de la entidad en un valor entre 701 SMLMV y 3.000 SMLMV. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor entre 701 SMLMV y 3.000 SMLMV.
1. Insignificante	• Impacto que afecte el presupuesto en un valor <700 SMLMV. • Pérdida de cobertura en la prestación de los servicios de le entidad entre el 1 y 5%. • Pago de indemnizaciones a terceros por acciones legales que pueden llegar a afectar el presupuesto total de la entidad en un valor <700 SMLMV. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <700 SMLMV.

Tabla 6. Escalas de Impacto cuantitativas

El análisis implica la consideración de las fuentes de riesgo, sus consecuencias positivas y negativas (la posibilidad de que dichas consecuencias puedan ocurrir) y los costos de su

posible afectación, para lo cual se establece la siguiente estructura:

COSTOS DE LA POSIBLE AFECTACION	**RIESGO INHERENTE**		
	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO

Tabla 7. Matriz de Riesgo Inherente

Costo de la posible afectación: Se determina teniendo en cuenta la tabla Nro. 5 Escalas de Impacto cuantitativas, cuya valoración debe corresponder al valor o ponderación otorgado al impacto en caso de llegarse a presentar la materialización del riesgo.

En caso de no lograrse cuantificar el riesgo, se relacionará que el mismo se calificará de forma cualitativa

Determinar Probabilidad: Debe ser medida bajo los criterios de la Tabla No 4.

Determinar el Impacto: Debe ser medido bajo los criterios de las Tablas No 5 o 6.

Nivel del riesgo: Enuncie el resultado de multiplicar la probabilidad y el impacto que puede causar la materialización del riesgo, a través de las tablas establecidas en cada caso y se define.

DEFINICIÓN DEL MAPA DE CALOR

Teniendo en cuenta las calificaciones de probabilidad e impacto obtenidas, se produce el Mapa de Calor de la Entidad en un plano cartesiano de 5 x 5, compuesto en su ordenada (eje Y) por la escala de la probabilidad de ocurrencia y en su abscisa (eje X) por la escala del impacto. A continuación se presenta la estructura del Mapa de Calor:

PROBABILIDAD					
Casi Seguro	*5*	*10*	*15*	*20*	*25*
Probable	4	8	12	16	20
Posible	3	6	9	12	15
Improbable	2	4	6	8	10
Rara Vez	1	2	3	4	5
	Insignificante	Menor	Moderado	Mayor	Catastrófico

IMPACTO

Gráfica 2. Mapa de Calor

Nivel del riesgo: es el resultado entre la probabilidad y el impacto que puede causar la materialización del riesgo, a través de las tablas establecidas en cada caso. Los colores indican el nivel de atención que se debe prestar a cada uno de los riesgos dependiendo de la zona en donde se encuentren ubicados, a continuación se presentan los niveles de atención aprobados por la Alta Dirección de la Entidad:

NIVEL DEL RIESGO RESIDUAL	NIVEL DE ATENCIÓN REQUERIDA
BAJA	Administrar mediante los controles y procedimientos establecidos operativamente
MODERADA	Responsabilidad de atención del líder de proceso
ALTA	Responsabilidad de atención del comité SISTEDA
EXTREMA	Requiere atención inmediata; Responsabilidad de atención de Dirección General y Consejo Directivo

Tabla 8. Matriz de Atención a los riesgos

ARTÍCULO 6. EVALUACIÓN DEL RIESGO

En la evaluación del riesgo se busca confrontar los resultados del análisis de riesgo inicial frente a la identificación de controles actuales, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL). El cual tiene como objetivo facilitar la toma de decisiones basada en el resultado del análisis, en donde se define cuáles de estos riesgos requieren de planes de acción, tratamiento y la prioridad de su implementación.

Los factores de calificación de controles relacionados en la tabla 9 se califican de acuerdo con las siguientes instrucciones:

Descripción controles actuales: Se diligencia el control que actualmente se implementa y/o ejecuta por parte del proceso para prevenir o mitigar el riesgo.

Naturaleza del control: Se diligencia el tipo de control Preventivo o Correctivo, teniendo en cuenta la siguiente descripción:

Controles Correctivos: Este tipo de control toma las acciones necesarias una vez materializado el riesgo y busca mejorar los demás controles si se determina que su funcionamiento no corresponde a las expectativas por las cuales fueron diseñados.

Controles Preventivos: Es el que actúa sobre las causas del riesgo o agentes generadores, con el fin de disminuir la probabilidad de ocurrencia del riesgo. En general, este tipo de controles son considerados como la primera barrera de seguridad que se establece para reducir un riesgo y comúnmente son implementados en asocio con otro tipo de controles porque no son suficientes por sí solos.

Manuales e instructivos para el manejo del control: Hace referencia respecto a si el control mencionado anteriormente se encuentra documentado mediante algún procedimiento, instructivo, formato, plan de acción y/o mejoramiento, protocolo, política, etc.

Calificación: Si el control se encuentra documentado, su calificación será de **15**, en caso de no estar documentado será de **0**

¿Está (n) definido (s) los responsables de la ejecución del control?: Hace referencia a, si en el proceso se tiene definido un responsable que se encargue de ejecutar o hacer seguimiento del control.

Calificación: Si el control cuenta con un responsable(s) su calificación será de **5**, en caso de que no cuente será de **0**.

Tipo de Controles implementados: Hace referencia al tipo de control que se está implementado, ya sea automático (mediante aplicativos tecnológicos) o manual (actividades operativas lideradas por personas).

Calificación: Si el control es manual su calificación será de **10**, en caso de que sea Automático su calificación será de **15.**

Frecuencia de seguimiento: Hace referencia a, si actualmente se realiza un seguimiento periódico a la ejecución del control.

Calificación**:** En caso de que la frecuencia sea adecuada, su calificación será de **15**, en caso de que no cuente, será de **0**.

Evidencia de la ejecución o seguimiento del control: Hace referencia a si el control cuenta con evidencia soporte de la gestión que se está realizando.

Calificación**:** En caso de que cuente con evidencia, su calificación será de **10**, en caso de que no cuente con evidencia, será de **0**.

Eficacia del control: Hace referencia a la satisfacción y efectividad que genera el control en lo que éste lleva de implementado.

Calificación**:** En caso de que sea efectivo el control, su calificación será de **30**, en caso de que no, será de **0**.

Teniendo en cuenta los factores anteriormente, se establece la siguiente estructura de valoración de controles en la cual se registrará el análisis a cada control identificado y de este modo, poder determinar el desplazamiento dentro de la Matriz de Evaluación de Riesgos.

VALORACIÓN DE LOS CONTROLES											
Descripción controles actuales	Naturaleza del control	¿El control se encuentra documentado? Si = 15 no = 0	¿Se encuentra definido un responsable del control o seguimiento?		Determinar el tipo de control		Frecuencia de seguimiento si = 15 no = 0	¿Existen evidencias del seguimiento?		¿Consideran que la herramienta ha sido efectiva? Si = 30 no = 0	Total calificación de controles
			Si = 5 no = 0	Cargo responsable	Automático Si = 15 no =0	Manual Si = 10 no = 0		Si = 10 no = 0	¿Cuál?		

Tabla 9. Matriz de Valoración de Controles

A través de la evaluación de controles establecidos en cada riesgo, se obtiene el nivel de **RIESGO RESIDUAL** calculando el promedio de cada factor para finalmente sumar el resultado de cada promedio obteniendo el resultado final de la evaluación de controles, el cual tiene el fin de identificar el desplazamiento del riesgo en su probabilidad o impacto según el siguiente rango de resultados:

RANGO DE CALIFICACION DE LOS CONTROLES	**DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO SE DESPLAZA EN LA MATRIZ DE EVALUACIÓN DEL RIESGO ASI:** **EN PROBABILIDAD AVANZA HACIA ABAJO EN IMPACTO AVANZA HACIA LA IZQUIERDA**
ENTRE 0 – 50	0
ENTRE 51 – 75	1
ENTRE 76 – 100	2

Tabla 10. Tabla rangos de controles. Metodología DAFP

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 entidad 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

Como tratamiento de los riesgos se pueden establecer diferentes circunstancias, tales como:

- Evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó.
- Tomar o incrementar el riesgo para perseguir una oportunidad.
- Retirar la fuente del riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con una varias de las partes, (incluyendo los contratos y la financiación del riesgo).
- Retener el riesgo mediante decisión informada.

Para el establecimiento de acciones de mitigación y/o fortalecimiento de los controles se establece la siguiente estructura:

ACCIONES	FECHA DE INICIO	FECHA DE FINALIZACIÓN

Tabla 11. Matriz acciones

Acciones: El proceso deberá proponer actividades que permitan fortalecer los controles existentes y contribuyan a mitigar el riesgo.

Fecha de inicio: Para dichas acciones se deberá establecer una fecha de inicio para las mismas.

Fecha de Finalización: Finalmente se debe establecer una fecha de cumplimiento para la acción, la cual será verificada en la etapa de monitoreo y revisión.

Elaboración del mapa de riesgos[1]: El mapa de riesgos es una representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa, como productos finales se obtienen:

Mapa institucional de riesgos: Contiene a nivel estratégico los riesgos a los cuales está expuesta la entidad, se alimenta con los riesgos que pueden afectar el cumplimiento de la misión institucional y objetivos de la entidad. En este mapa se deberán incluir los riesgos identificados como posibles actos de corrupción, en cumplimiento del artículo 73 de la Ley 1474

[1]Tomado de la guía para la administración del riesgo del Departamento Administrativo de la Función Pública- Diciembre 2014.

de 2011.

Mapa de riesgos por procesos: Recoge los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.
El énfasis del mapa institucional está en los riesgos altos y extremos de cada proceso. Todas las acciones contempladas dentro del mapa, unido a la información reportada por los indicadores debe suministrar la información requerida para el seguimiento respectivo a los mapas.

ARTÍCULO 7. MONITOREO Y REVISIÓN.

En el proceso de monitoreo y revisión se tienen en cuenta todos los aspectos del proceso para la gestión del riesgo, que ayuden a garantizar que los controles y las acciones de mitigación sean eficaces y eficientes. El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

Responsabilidad del monitoreo

Dueños de Procesos: Encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso, de acuerdo con la periodicidad establecida en la política de administración del riesgo. Durante la aplicación de las acciones de seguimiento cada dueño de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplirán.

Oficina de Planeación y Oficina de Control Interno: realizarán el monitoreo y seguimiento respectivamente de acuerdo a lo establecido en la Tabla 1. Responsabilidades frente a la administración del riesgo

Periodicidad del seguimiento

Se realizará el monitoreo trimestral en el comité Institucional de Gestión y Desempeño, presentado por la Oficina de Planeación de acuerdo al seguimiento realizado por los dueños de proceso.

Para riesgos asociados a posibles actos de corrupción, se debe dar cumplimiento a las fechas establecidas por la guía de la Secretaría de transparencia, denominada “Guía para la gestión del riesgo de corrupción 2015”; para los riesgos de gestión ubicados en las diferentes zonas de riesgo residual, se tomarán en cuenta las fechas establecidas en la política de riesgos institucional. Las frecuencias de medición definidas no deben superar los tres meses, de forma que permitan que el seguimiento realizado sea base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

De igual manera, en el ejercicio de autoevaluación trimestral se deberán monitorear y revisar los indicadores de gestión establecidos para los planes de acción y para los riesgos, permitiendo conocer el estado de ejecución actual de dichos planes. Es por esto que a continuación se presenta la metodología para el establecimiento de los indicadores de gestión de riesgos de la Entidad.

Indicadores De Gestión Del Riesgo[2]:

Para el establecimiento de los indicadores se debe tener en cuenta que éstos son una relación entre dos o más variables, a partir de la cual se registra, procesa y presenta información relevante con el fin de medir el avance o retroceso en el logro de un determinado objetivo en un periodo de tiempo determinado, ésta debe ser verificable objetivamente, la cual al ser comparada con algún nivel de referencia (denominada línea base), puede estar señalando una desviación sobre la cual se pueden implementar acciones correctivas o preventivas según el caso.

Con el fin de formular adecuadamente los indicadores se deben tener en cuenta las siguientes características:

CARACTERÍSTICAS	DESCRIPCIÓN
Pertinencia	Debe referirse a los procesos y productos esenciales que desarrolla cada institución.
Independencia	No condicionado a factores externos, tales como la situación general del país o la actividad conexa de terceros (públicos o privados).
Costo	La obtención de la información para la elaboración del indicador debe ser a costo razonable.
Confiabilidad	Digno de confianza independiente de quién realice la medición.
Simplicidad	Debe ser de fácil comprensión, libre de complejidades.
Oportunidad	Debe ser generado en el momento oportuno dependiendo del tipo de indicador y de la necesidad de su medición y difusión.
No Redundancia	Debe ser único y no repetitivo.
Focalizado en áreas controlables	Focalizado en áreas susceptibles de corregir en el desempeño de los organismos públicos generando a la vez responsabilidades directas en los funcionarios y el personal.
Participación	Su elaboración debe involucrar en el proceso a todos los actores relevantes, con el fin de asegurar la legitimidad y reforzar el compromiso con los objetivos e indicadores resultantes. Esto implica además que el indicador y el objetivo que pretende evaluar sea lo más consensual posible al interior de la organización.

[2]Definiciones y metodología tomada de la Guía para la construcción y análisis de indicadores de Gestión del Departamento Administrativo de la Función Pública – Versión 3 Noviembre de2015.

CARACTERÍSTICAS	DESCRIPCIÓN
Disponibilidad	Los datos básicos para la construcción del indicador deben ser de fácil obtención sin restricciones de ningún tipo.
Sensibilidad	El indicador debe ser capaz de poder identificar los distintos cambios de las variables a través del tiempo.

Tabla 12. Características de indicadores

Para el establecimiento de los indicadores de gestión se establece la siguiente estructura en la matriz de riesgos:

INDICADOR PARA EL PLAN DE ACCIÓN / INDICADOR PARA EL RIESGO					
Nombre del indicador	Formula de medición del indicador	Tipo de indicador	Periodo de medición	Meta esperada del indicador	Resultado del indicador

Tabla 13. Matriz de Indicadores de gestión para los planes de acción

Nombre del Indicador: Se asigna un nombre descriptivo para el indicador, el cual debe tener relación con el riesgo y/o plan de acción.

Formula de Medición del Indicador: Se establecen las variables de medición para obtener los resultados esperados del indicador teniendo el tipo de indicador que se desea emplear.

Periodo de Medición: Se debe establecer un periodo de tiempo para verificar la ejecución y cumplimiento del indicador.

Meta Esperada del Indicador: Establecer un valor en porcentaje y/o valor esperado del cumplimiento del indicador creado.

Resultado del Indicador: Este resultado debe ser actualizado trimestralmente, de acuerdo a los avances presentados por cada proceso.

De acuerdo con el seguimiento trimestral realizado es importante considerar al final de cada vigencia si los Mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo. Para poder determinarlo se analizará si no se han presentado hechos significativos como son:

- Riesgos materializados relacionados con posibles actos de corrupción.
- Riesgos de gestión materializados en cualquiera de los procesos.
- Observaciones o hallazgos por parte de la Oficina de Control Interno o bien por parte de un ente de control, respecto de la idoneidad y efectividad de los controles.
- Cambios importantes en el entorno que puedan generar nuevos riesgos.

No obstante, los mapas de riesgos deben ser flexibles y permitir cambios cuando se requieran.

Estos aspectos deben ser considerados para posibles ajustes o cambios sobre los lineamientos establecidos en la política de riesgos institucional, para fortalecer la administración del riesgo en la entidad.

ARTÍCULO 8. REPORTE DE RIESGOS MATERIALIZADOS

Aquellos riesgos de gestión que se materialicen deberán ser reportados al Líder de proceso para proceder con las acciones correctivas correspondientes, de igual forma los riesgos de corrupción deberán ser reportados a la Alta Dirección, tal como se muestra en la tabla No. 14, para proceder con las acciones pertinentes:

Tipo de Riesgo / **Detectado por**	**Riesgo de corrupción**	**Riesgo de Gestión (Zona Extrema, alta o moderada)**	**Riesgo de Gestión (Zona Baja)**
Oficina de Control Interno	1. Convocar al Comité de coordinación de control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. 3. Facilitar el inicio de las acciones correspondientes con el dueño del proceso, para revisar el mapa de riesgos y sus controles asociados. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.	1. Informar al dueño del proceso sobre el hecho encontrado. 2. Orientar al dueño del proceso para que realice la revisión, análisis y acciones Correspondiente para resolver el hecho. 3. Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. 4. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.	Informar al dueño del proceso sobre el hecho. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucionales.

Tipo de Riesgo / **Detectado por**	**Riesgo de corrupción**	**Riesgo de Gestión (Zona Extrema, alta o moderada)**	**Riesgo de Gestión (Zona Baja)**
Líder del proceso u otro(s) funcionario(s) que participa(n) O interactúa(n) con el proceso	1. Informar a la Dirección sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo. 3. Iniciar con las acciones correctivas necesarias. 4. Realizar el análisis de causas y determinar acciones preventivas y de mejora. 5. Análisis y actualización del mapa de riesgos.	1. Tomar las acciones correctivas necesarias, dependiendo del riesgo materializado. 2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora. 3. Analizar y actualizar el mapa de riesgo. 4. Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.	Aplicar las orientaciones de la política de riesgos institucionales (verificar los niveles de aceptación del riesgo

Tabla 14. Acciones en caso de Materialización de los Riesgos

Es de vital importancia validar y registrar la pérdida como consecuencia de la materialización del riesgo. Una vez validada la información de la pérdida, el Líder del Proceso procede a su reporte en módulo de riesgos de la SUITE VISION EMPRESARIAL, en este se debe realizar la descripción del evento y adjuntar los respectivos soportes. El reporte de las pérdidas debe realizarse de forma inmediata al momento de su identificación, si este es considerado como de impacto alto; en caso de que la pérdida no sea considerada de importancia relevante, se puede reportar al finalizar la semana en que se materializó el riesgo.

ARTÍCULO 9. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo. Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia,

con el fin de que porten su conocimiento en la identificación, análisis y valoración del riesgo.
La entidad cuenta con la herramienta Suite Visión Empresarial, en donde cada dueño de proceso verifica el perfil de los riesgos, los cuales deberán ser presentados en la autoevaluación trimestral.

TÍTULO 3. ALINEACION DEL MANUAL DE ADMINISTRACION DEL RIESGO

ARTÍCULO 10. POLÍTICAS DE LUCHA CONTRA LA CORRUPCIÓN Y DE EFICIENCIA ADMINISTRATIVA

Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos. La Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción.

Entendiendo que los riesgos de corrupción se convierten en una tipología de riesgos que debe ser controlada por la entidad, éstos deben incorporarse en primera instancia en el mapa de riesgos del proceso, sobre el cual se han identificado, de modo tal que el dueño del mismo pueda realizar el seguimiento correspondiente, en conjunto con los riesgos de gestión propios del proceso.

En este sentido, es importante precisar que el seguimiento a los riesgos de corrupción en primer lugar es responsabilidad de los dueños de los procesos en los cuales fueron identificados, así mismo de la oficina de planeación quien realiza seguimiento y finalmente de la Oficina de Control Interno quien es la encargada de evaluar las efectividad de los controles y determinar si se han materializado o no este tipo de riesgos.

En segunda instancia los riesgos relacionados con posibles actos de corrupción deben consolidarse dentro del mapa de riesgos institucional, con el fin de realizar el monitoreo respectivo por parte de la Oficina de Control Interno o quien haga sus veces, esto por tratarse de riesgos críticos frente al cumplimiento de la misión, visión y objetivos institucionales. Estas acciones permiten que la Administración o Gestión del Riesgo sea sistémica para la entidad y sea analizado en conjunto para la toma de decisiones en los diferentes escenarios para tal fin.

Teniendo en cuenta que la Secretaría de Transparencia de la Presidencia de la República en su guía “Guía para la gestión del riesgo de corrupción 2015” establece dentro de su metodología para los riesgos de corrupción niveles diferentes frente al análisis y valoración del riesgo, al incorporar estos riesgos a los mapas por proceso e institucional, será necesario adaptar e integrar el formato que dicha guía contiene, sin desconocer los lineamientos generales allí establecidos.

ARTÍCULO 11. METODOLOGÍA PARA LOS RIESGOS DE CORRUPCIÓN

Casur adopta la metodología para la Administración del Riesgo en todas sus etapas (Grafica 1, página 18) con el fin de gestionar los riesgos de corrupción, sin embargo en la etapa de análisis de los riesgos, se toma como referencia las escalas de valoración de Probabilidad e Impacto de la Guía para la Gestión de Riesgo de Corrupción-Versión 2015 del Departamento Administrativo de la Función Pública, ya que tratándose de riesgos de corrupción el impacto siempre será negativo por lo tanto la valoración del Riesgo Inherente será realizada bajo criterios específicos.

Con el fin de otorgar valoración a la probabilidad para los riesgos de corrupción se establecen los siguientes niveles:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	**Rara vez**	**Excepcional** Ocurre en excepcionales	No se ha presentado en los últimos 5 años.
2	**Improbable**	**Improbable** Puede Ocurrir	Se presentó 1 vez en los últimos 5 años.
3	**Posible**	**Posible** Es posible que suceda.	Se presentó 1 vez en los últimos 2 años
4	**Probable**	**Es probable** Ocurre en la mayoría de los casos	Se presentó 1 vez en el último año.
5	**Casi seguro**	**Es muy seguro** El evento ocurre en la mayoría de las circunstancias	Se ha presentado más de 1 vez al año

Tabla 15. Escalas de probabilidad del riesgo de corrupción

Para la medición del Impacto de los riesgos de corrupción se utiliza la siguiente tabla:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
5	**MODERADO**	**Afectación parcial al proceso y a la dependencia** Genera a medianas consecuencias para la entidad.
10	**MAYOR**	**Impacto negativo de la Entidad** Genera altas consecuencias para la entidad.
20	**CATASTRÓFICO**	**Consecuencias desastrosas sobre el sector** Genera consecuencias desastrosas para la entidad.

Tabla 16. Escalas de Impacto del riesgo de corrupción

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines y objetivos de la entidad. Para facilitar la asignación del puntaje de impacto se debe responder a la siguiente encuesta:

No.	PREGUNTA	RESPUESTA	
		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 o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
Total preguntas afirmativas:			
Total preguntas negativas:			

Tabla 17. Encuesta para determinar el Impacto

Según el resultado de la encuesta se logra identificar el valor del impacto real del riesgo teniendo en cuenta lo siguiente:

Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto Moderado.

Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.

Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto Catastrófico.

NIVEL DEL RIESGO	TRATAMIENTO REQUERIDO
BAJA	Los riesgos de corrupción de las zonas baja se encuentran en un nivel que puede eliminarse o reducirse fácilmente con los controles establecidos en la entidad.

MODERADA	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Baja o eliminarlo. **Nota** En todo caso se requiere que las entidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.
ALTA	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Moderada, Baja o eliminarlo. **Nota** En todo caso se requiere que las entidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.
EXTREMA	Los riesgos de corrupción de la Zona de Riesgo Extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección. **Nota** En todo caso se requiere que las entidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.

Tabla 18. Matriz de Tratamiento a los riesgos de corrupción

Posteriormente para determinar el riesgo Inherente se realiza a través del cruce de los resultados obtenidos de la probabilidad y del impacto, a través de una multiplicación (puntaje del descriptor de la probabilidad por el puntaje del descriptor del impacto), ubicando el riesgo en el siguiente mapa de calor:

PROBABILIDAD	Moderado	Mayor	Catastrófico
Casi Seguro	25	50	100
Probable	20	40	80
Posible	15	30	60
Improbable	10	20	40
Rara Vez	5	10	20

IMPACTO

Gráfica 3. Mapa de Calor Corrupción

ARTÍCULO 12. METODOLOGÍA PARA LOS RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Información pública reservada	Alta (a)	Alta (1)
Información pública clasificada	Media (m)	Media (2)
Información pública	Baja (b)	Baja (3)
No clasificada	No clasificada	No clasificada

Tabla 19. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 20. Niveles de Clasificación

Casur atendiendo los lineamientos del Modelo de Seguridad y Privacidad de GEL en lo referente a la protección de la confidencialidad, integridad y disponibilidad de la información bajo la responsabilidad de la Entidad y cumpliendo con el MSPI (Modelo de seguridad y privacidad de la información) adopta la metodología para la Administración del Riesgo en todas sus etapas (Grafica 1, página 18) sin embargo en la etapa de análisis de los riesgos, se toma como referencia la definida en la guía de gestión de riesgos de seguridad y privacidad de la información del MINTIC basadas la norma ISO 27005.

Identificación del riesgo: El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

Identificación de los activos: Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación

de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. **Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.**

Identificación de las amenazas: Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas), algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados, a continuación se describen una serie de amenazas comunes.

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosion, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcanoes	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	

TIPO	AMENAZA	ORIGEN
Compromiso de la información	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
	Espionaje remoto	
	Escucha encubierta	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	
Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	
	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Tabla 21: Amenazas Comunes Fuente Guía de gestión de riesgos MINTIC

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería Ingeniería Social Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad Intrusión en el sistema

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/Terrorismo Guerra de la información Ataques contra el sistema DoS Penetración en el sistema Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Tabla 22: Amenazas Humanas Fuente Guía de gestión de riesgos MINTIC

Identificación de controles existentes

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo, se deberían considerar en la misma forma que aquellos que ya están implementados

Un control existente planificado se podría calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.
- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas

A continuación se relacionan los controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

Núm.	Nombre	Selección / Excepción	Descripción / 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		
A.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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.14.1.1	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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
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.

Tabla 23: Controles Fuente Guía de gestión de riesgos MINTIC

Identificación de las vulnerabilidades

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de

amenazas comunes, la lista de inventario de activos y el listado de controles existentes.
Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

NOTA: La sola presencia de una vulnerabilidad no causa daños por si misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación se enunciarán vulnerabilidades conocidas y métodos para la valoración de la misma.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
SOFTWARE	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
RED	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
INFORMACION FISICA, DIGITAL	Incumplimiento de los programas de conservación documental	Perdida documentos
	Almacenamiento y archivo inadecuado	Perdida documentos
	Uso documentos no controlados por el sistema gestión integral	Incumplimiento requisitos del sistema de gestión integral
	Aplicación inadecuada de las tablas de retención documental	Error en la disposición final
	Incumplimiento de procedimientos documentales	Incumplimiento de los preceptos normativos
	Organización inadecuada de archivos digitales sin la aplicación de las TRD	Brindar información erronea
	Ausencia copias de respaldo Back up	Continuidad del negocio
ORGANIZACIÓN	procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditoria	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos

Tabla 24: Vulnerabilidades Fuente Guía de gestión de riesgos MINTIC

ARTÍCULO 13. METODOLOGIA PARA LA IDENTIFICACION DE LOS PELIGROS Y LA VALORACION DE LOS RIESGOS EN SEGURIDAD Y SALUD EN EL TRABAJO.

Para la identificación de los peligros y la valoración de los riesgos se llevaran a cabo las siguientes acciones

Reconocimiento del proceso productivo:
El proceso productivo que se desarrolla es: Empresas dedicadas a actividades ejecutivas de la administración pública en general, incluye ministerios, órganos, organismos y dependencias administrativas en los niveles central, regional y local.

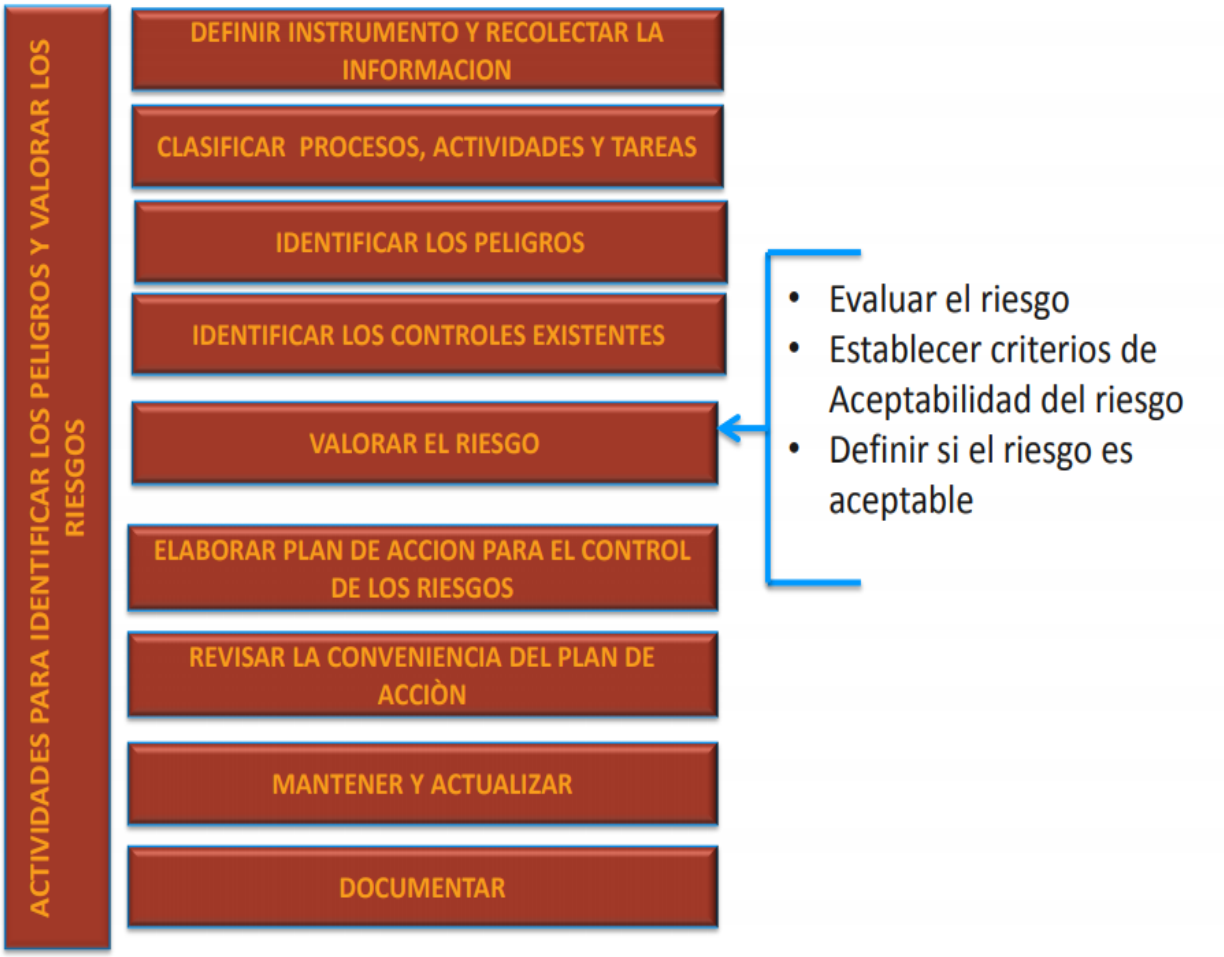
- Principales materias primas utilizadas: Papel, Carpetas, Sistemas de Información.
- Productos que se fabrican: Servicios
- Subproductos que se generan: Servicios
- Máquinas y herramientas que se utilizan: Computadores, Scanner, impresoras,

Archivadores, Escritorios, herramientas manual de oficina (cosedora, grapadora, quitaganchos, lapiceros).

Identificación de peligros

Para realizar la identificación de peligros, evaluación y valoración de los riesgos y determinación de controles en CAJA DE SUELDOS DE RETIRO DE LA POLICIA NACIONAL, se elaboró una matriz de identificación de peligros, valoración de riesgos y determinación de controles utilizando la guía GTC 45/2012 – Guía para el diagnóstico de condiciones de trabajo o matriz de identificación y valoración de riesgos.

El procedimiento establecido para realizar la identificación de los peligros y la valoración de los riesgos en la Entidad es tomado de GTC 45 /2012 se describe a continuación:



Gráfica 4 Actividades a seguir en la identificación de los peligros y valoración de los riesgos
Fuente: GTC45/2012

A partir del conocimiento de la actividad económica de la entidad, los accidentes presentados en años anteriores, el proceso productivo y una inspección de las áreas de trabajo, se realiza un inventario de los peligros a los que están expuestos los servidores públicos, contratistas, personal de comisión y/o visitantes, con base en la clasificación de los factores de riesgo sugerida por la GTC 45.

Teniendo en cuenta el nivel de daño que puede generar en las personas. A continuación se proporciona el ejemplo de niveles de daño (GTC45/2012-TABLA 25 Descripción de los Niveles de Daño).

CATEGORÍA DEL DAÑO	DAÑO LEVE	DAÑO MODERADO	DAÑO EXTREMO
SALUD	Molestias e irritación (ej.: dolor de cabeza), enfermedad temporal que produce malestar (ej.: diarrea).	Enfermedades que causan enfermedad temporal, (ej.: pérdida temporal de la audición, dermatitis, asma, desordenes de las extremidades superiores.	Enfermedades agudas o crónicas, que generan incapacidad permanente, parcial, invalides o muerte.
SEGURIDAD	Lesiones superficiales, heridas de poca profundidad, contusiones irritaciones de ojo por material particulado.	Laceraciones heridas profundas, quemaduras de primer grado, conmoción cerebral, esguinces graves, fracturas de huesos cortos.	Lesiones que generan amputaciones, fracturas de huesos largos, trauma cráneo encefálico, quemaduras de segundo y tercer grado, alteraciones severas de mano, de columna vertebral con compromiso de la medula espinal, oculares que comprometan el campo visual, disminuyan la capacidad auditiva.

Tabla 25. Descripción de los Niveles de Daño

Identificación de controles existentes: Se identifican los controles existentes para cada uno de los peligros identificados y clasificados en: Fuente, Medio e Individuo.

Se consideran los controles administrativos que se han implementado para disminuir el riesgo, como: Inspecciones, Ajustes a procedimientos, horarios de Trabajo, entre otros.

Valorar el Riesgo: La valoración del Riesgo en GTC45/2012 incluye:

La evaluación del riesgo teniendo en cuenta la suficiencia de controles existentes y la definición de criterios de aceptabilidad del riesgo, la decisión de si son aceptables o no, con base en

criterios definidos.

En esta evaluación se tienen en cuenta para aceptar el riesgo los siguientes aspectos:

- Cumplimiento de Requisitos legales.
- Política de Seguridad y Salud en el Trabajo.
- Objetivos y metas de la Entidad.
- Aspectos operacionales, técnicos, financieros, sociales y otro.

Evaluación del riesgo:

La evaluación de los riesgos corresponde al proceso de determinar la probabilidad de que ocurran eventos específicos y la magnitud de sus consecuencias, mediante el uso sistemático de la información disponible.

Luego de identificados los peligros se realiza su estimación mediante la calificación de la probabilidad vs la consecuencia, lo que permite ubicar los peligros dentro de una escala o nivel del riesgo, como se observa en la matriz que se presenta para evaluar el nivel de riesgo (NR), se aplica lo siguiente:

NR = NP x NC

Dónde: NP = Nivel de probabilidad

NC = Nivel de consecuencia

A su vez, para determinar el NP se requiere:

NP= ND x NE

Dónde: ND = Nivel de deficiencia

NE = Nivel de exposición

Para determinar el nivel de deficiencia (ND) se utiliza la tabla 26

NIVEL DE DEFICIENCIA	VALOR DE ND	SIGNIFICADO
Muy Alto (MA)	10	Se ha(n) detectado peligro(s) que determina(n) como posible la generación de incidentes o consecuencias muy significativas, o la eficacia de medidas preventivas existentes respecto al riesgo es nula o no existe, o ambos.
Alto (A)	6	Se ha(n) detectado algún(os) peligro(s) que pueden dar lugar a consecuencias significativa(s), o la eficacia de medidas preventivas existentes es baja, o ambos.

Medio (M)	2	Se han detectado peligros que pueden dar lugar a consecuencias poco significativas o de menor importancia, o la eficacia de medidas preventivas existentes es moderada, o ambos.
Bajo (B)	No se Asigna Valor	No se ha detectado consecuencia alguna, o la eficacia de medidas preventivas existentes es alta, o ambos. El riesgo está controlado. Estos peligros se clasifican directamente en el nivel de riesgo y de intervención cuatro (IV) Véase tabla 8.

Tabla 26: Determinación del Nivel de Deficiencia

Nota: Para determinar el nivel de deficiencia para los peligros psicosociales la Entidad utilizara la metodología nacional disponible (aplicación Batería de riesgo psicosocial Universidad Javeriana-Min protección Social).

Para determinar el NE se aplican los criterios establecidos en GTC45/2012 TABLA 27.

NIVEL DE EXPOSICIÓN	VALOR DE NE	SIGNIFICADO
Continua (EC)	4	La situación de exposición se presenta sin interrupción o varias veces con tiempo prolongado durante la jornada laboral.
Frecuente (EF)	3	La situación de exposición se presenta varias veces durante la jornada laboral por tiempos cortos.
Ocasional (EO)	2	La situación de exposición se presenta alguna vez durante la jornada laboral y por un periodo de tiempo corto.
Esporádica (EE)	1	La situación de exposición se presenta de manera eventual.

Tabla 27. Determinación del nivel de exposición

Para determinar el nivel de probabilidad (NP) se combinaron los resultados de las tablas 26 y 27, en la tabla 28.

NIVELES DE PROBABILIDAD		NIVEL DE EXPOSICIÓN (NE)			
		4	3	2	1
Nivel de deficiencia (ND)	10	MA – 40	MA – 30	A –20	A - 10
	6	MA – 24	A – 18	A – 12	M - 6
	2	M – 8	M – 6	B – 4	B – 2

Tabla 28. Determinación del nivel de probabilidad

El resultado de la tabla 28, se interpretó de acuerdo con el significado que aparece en la tabla 28.

NIVEL DE PROBABILIDAD	VALOR DE NP	SIGNIFICADO
Muy Alto (MA)	Entre 40 y 24	Situación deficiente con exposición continua, o muy deficiente con exposición frecuente. Normalmente la materialización del riesgo ocurre con frecuencia.
Alto (A)	Entre 20 y 10	Situación deficiente con exposición frecuente u ocasional, o bien situación muy deficiente con exposición ocasional o esporádica. La materialización del riesgo es posible que suceda varias veces en la vida laboral.
Medio (M)	Entre 8 y 6	Situación deficiente con exposición esporádica, o bien situación mejorable con exposición continuada o frecuente. Es posible que suceda el daño alguna vez.
Bajo (B)	Entre 4 y 2	Situación mejorable con exposición ocasional o esporádica, o situación sin anomalía destacable con cualquier nivel de exposición. No es esperable que se materialice el riesgo, aunque puede ser concebible.

Tabla 29. Significado de los diferentes niveles de probabilidad

Luego se determinó el nivel de consecuencias según los parámetros de la tabla 30.

NIVEL DE CONSECUENCIAS	NC	SIGNIFICADO
		DAÑOS PERSONALES
Mortal o Catastrófico (M)	100	Muerte (s)
Muy grave (MG)	60	Lesiones o enfermedades graves irreparables (Incapacidad permanente parcial o invalidez).
Grave (G)	25	Lesiones o enfermedades con incapacidad laboral temporal (ILT).
Leve (L)	10	Lesiones o enfermedades que no requieren incapacidad.

Tabla 30. Determinación del nivel de consecuencias

Los resultados de las tablas 28 y 29 se combinaron en la tabla 30 para obtener el nivel de riesgo, el cual se interpretó de acuerdo con los criterios de la tabla 31.

NIVEL DE RIESGO NR = NP x NC		**NIVEL DE PROBABILIDAD (NP)**			
		40-24	20-10	8-6	4-2
Nivel de consecuencias (NC)	100	I 4000-2400	I 2000-1200	I 800-600	II 400-200
	60	I 2400-1440	I 1200-600	II 480-360	II 240 / III 120
	25	I 1000-600	II 500 – 250	II 200-150	III 100- 50
	10	II 400-240	II 200 / III 100	III 80-60	III 40 / IV 20

Tabla 31. Determinación del nivel de riesgo

NIVEL DE RIESGO	**VALOR DE NR**	**SIGNIFICADO**
I	4000-600	Situación crítica. Suspender actividades hasta que el riesgo esté bajo control. Intervención urgente.
II	500 – 150	Corregir y adoptar medidas de control de inmediato.
III	120 – 40	Mejorar si es posible. Sería conveniente justificar la intervención y su rentabilidad.
IV	20	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejoras y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es aceptable.

Tabla 32. Significado del nivel de riesgo

Decidir si el riesgo es aceptable o no: Una vez determinado el nivel de riesgo, se decidió cuáles riesgos son aceptables y cuáles no. La clasificación de la aceptabilidad del riesgo se muestra en la tabla 33.

Para hacer esto, la Entidad debe establecer los criterios de aceptabilidad, con el fin de proporcionar una base que brinde consistencia en todas sus valoraciones de riesgos. Esto debe incluir la consulta a las partes interesadas y debe tener en cuenta la legislación vigente.

NIVEL DE RIESGO	**SIGNIFICADO , EXPLICACIÓN**	
I	No Aceptable	Situación crítica corregir urgente
II	No Aceptable o Aceptable con control específico	Corregir o adoptar medidas de control
III	Mejorable	Mejorar el control existente
IV	Aceptable	No intervenir, salvo que un análisis más preciso lo justifique.

Tabla 33. Aceptabilidad del riesgo

Al aceptar un riesgo específico, se tiene en cuenta el número de expuestos y las exposiciones

a otros peligros, que pueden aumentar o disminuir el nivel de riesgo en una situación particular.

Plan de acción para el control de riesgos.
Los niveles de riesgo, como se muestra en la Tabla 31, forman la base para decidir si se requiere mejorar los controles y el plazo para la acción. Igualmente muestra el tipo de control y la urgencia que se debería proporcionar al control del riesgo. El resultado de una valoración de los riesgos debería incluir un inventario de acciones, en orden de prioridad, para crear, mantener o mejorar los controles.

Se tienen en cuenta los siguientes criterios:

Número de servidores públicos expuestos: importante tenerlo en cuenta para identificar el alcance del control a implementar.

Peor consecuencia: aunque se han identificado los efectos posibles, se debe tener en cuenta que el control a implementar evite siempre la peor consecuencia al estar expuesto al riesgo.

Existencia requisito legal asociado: se debe establecer si existe o no un requisito legal específico a la tarea que se está evaluando para tener parámetros de priorización en la implementación de las medidas de intervención.

Medidas de intervención: Se consideran la reducción de los riesgos de acuerdo a la siguiente jerarquización:

Eliminación: Modificar un diseño para eliminar el peligro.

Sustitución: Reemplazar por un material menos peligroso o reducir la energía del Sistema.

Controles de ingeniería: Instalar sistemas de ventilación, protección para las maquinas, enclavamientos, cerramientos acústicos etc.

Controles administrativos: señalización, advertencias (instalación de alarmas, procedimientos de seguridad, inspecciones de los equipos, controles de acceso, capacitación del personal)

Equipos y elementos de protección personal.

Al aplicar un control determinado se deberían considerar los costos relativos, los beneficios de la reducción de riesgos, y la confiabilidad de las opciones disponibles.

Una vez que la organización haya determinado los controles, ésta puede necesitar priorizar sus acciones para implementarlos. Para priorizar las acciones, se debería tener en cuenta el potencial de reducción de riesgo de los controles planificados.(GTC45)

Puede ser preferible que las acciones que abordan una actividad de alto riesgo u ofrecen una reducción considerable de éste, tengan prioridad sobre otras acciones que solamente ofrecen un beneficio limitado de reducción del riesgo.(GTC45)

Priorización de riesgos

La priorización de los factores de riesgo, se realiza de acuerdo a la valoración obtenida en el grado de peligrosidad, siendo:

Alto: La calificación más alta otorgada a un riesgo y que nos indica que este, se debe atender a corto plazo.

Medio: Esta calificación nos indica que el riesgo debe ser atendido en un periodo de tiempo a mediano plazo.

Bajo: Es la calificación más baja que se le da a un riesgo, no significando esto que sea menos importante; pero sí que se pueden ejecutar acciones correctivas a largo plazo. De acuerdo con lo anterior, a continuación se presenta la priorización de los riesgos:

Metodología de acuerdo a GTC45/2012

Proceso	Zona/Lugar	Actividad	Tareas	Rutinaria (Sí o No)	Peligro		Efectos posibles	Controles existentes		
					Descripción	Clasificación		Fuente	Medio	Trabajador

Tabla 34. Identificación de Peligros

Evaluación del Riesgo							Valoración del Riesgo
Nivel de deficiencia	Nivel de exposición	Nivel de probabilidad (NP=ND x NE)	Interpretación del nivel de probabilidad	Nivel de consecuencia	Nivel de riesgo: (NR=NPxNC)	Interpretación del nivel de riesgo NR	Aceptabilidad del riesgo

Tabla 35. Valoración de Riesgos

Criterios para establecer controles		
Nro. De Expuestos	Peor Consecuencia	Existencia Requisito Legal Específico Asociado (Si o No)

Tabla 36. Criterios para valoración del riesgo

.**Medidas de intervención**				
Eliminación (E)	Sustitución (S)	Controles de Ingeniería (CI), Controles Administrativo(CA), Advertencia (A)	Señalización (S)	Elementos de Protección Personal (EPP)

Tabla 37. Determinación de Controles

Mantenimiento y actualización

Es importante que el empleador recuerde que el Decreto 1072 de 2015 establece las directrices de obligatorio cumplimiento para implementar el Sistema de Gestión de la Seguridad y Salud en el Trabajo y mantener actualizada la identificación de los peligros, evaluación y valoración de los riesgos para lo cual se basara en el tratamiento de los riesgos implementados, los cambios en el proceso y la legislación.

La determinación de la frecuencia se puede dar por alguno o varios de los siguientes aspectos:

La necesidad de determinar si los controles para el riesgo existentes son eficaces y suficientes.

- La necesidad de responder a nuevos peligros.
- La necesidad de responder a los cambios que la propia Entidad ha llevado a cabo.
- La necesidad de responder a retroalimentación de las actividades de seguimiento, investigación de incidentes, situaciones de emergencia o los resultados de las pruebas de los procedimientos de emergencia.
- Cambios en la legislación.
- Factores externos, por ejemplo, problemas de Seguridad y Salud en el Trabajo que se presenten.
- Avances en las tecnologías de control.
- La diversidad cambiante en la fuerza de trabajo, incluidos los contratistas.

Las revisiones periódicas pueden ayudar a asegurar la consistencia en las valoraciones de los riesgos llevadas a cabo, por diferente personal, en diferentes momentos. Donde las condiciones hayan cambiado o haya disponibles mejores tecnologías para manejo de riesgos, se deberían hacer las mejoras necesarias.

No es necesario llevar a cabo nuevas valoraciones de los riesgos cuando una revisión puede demostrar que los controles existentes o los planificados siguen siendo eficaces

ARTÍCULO 14. ALINEACIÓN CON EL MANUAL PARA LA IDENTIFICACIÓN Y COBERTURA DEL RIESGO EN LOS PROCESOS DE CONTRATACIÓN (AGENCIA NACIONAL PARA LA CONTRATACIÓN PÚBLICA)

La entidad debe articular la metodología de este manual con la administración del riesgo, proporcionando un mayor nivel de conocimiento y certeza de los procesos de contratación, mejorar la planeación de contingencias, incrementar el grado de confianza entre las partes y reducir la posibilidad de litigios.

ARTÍCULO 15. IDENTIFICACIÓN DE RIESGOS A LOS PROYECTOS

Los aspectos relacionados con la identificación del riesgo a los proyectos que desarrolla la entidad, deben ser incorporados en su gestión del riesgo institucional. Lo anterior de acuerdo al Decreto 943 de 2014 “Por el cual se actualiza el Modelo Estándar de control Interno MECI”, en el módulo de control a la planeación y gestión, sobre el desarrollo de metodologías que permitan ejercer el control sobre los proyectos.

TÍTULO 4. MARCO LEGAL

A continuación se presentan las normas establecidas, para la Administración del Riesgo, en las entidades públicas:

Norma	Contenido
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. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Norma	Contenido
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno
Decreto 2145 de1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8º. de la ley 1474 de 2011)
Directiva presidencial 09 de 1999	Lineamientos para la implementación de la política de lucha contra la corrupción.
Decreto 2593 del 2000	Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999
Decreto 1537 de 2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.
Decreto 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) “establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder”. Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades
Ley 1474 de 2011	Estatuto Anticorrupción. Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.
Decreto 4170 de 2011	Por el cual se crea la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente–
Decreto 2482 de 2012	Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión
Decreto 943 de 2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)

Tabla 38 Marco Normativo

.

Norma técnica, estándares internacionales y documentos asociados:

Estándar internacional ISO 31000:2009, Principios y Directrices.

Estándar internacional IEC/ FDIS 31010:2009 – Técnicas para la valoración de riesgos. Norma Técnica de Calidad en la Gestión Pública NTGP 1000:2009

Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano Presidencia de la República.

Guía para la administración del riesgo Departamento Administrativo de la Función Pública.

Guía para la gestión del riesgo de corrupción 2015 Presidencia de la República.

Decreto 1499 de 2017 por medio del cual se actualizó el Modelo Integrado de Planeación y Gestión

Manual Operativo del Modelo Integrado de Planeación y Gestión

Resolución 6554 del 05 de agosto de 2014, por el cual se crea el comité institucional de desarrollo administrativo de CASUR y se dictan otras disposiciones.

Resolución 402 del 15/02/16, “Por la cual, por la cual se deroga la Resolución 1129 del 28 de marzo de 2007 y se adopta el Manual de Administración del Riesgo de la Caja de Sueldos de Retiro de la Policía Nacional”.

Guía Técnica Colombiana GTC 45 V2 2012 Icontec Internacional, Consejo Colombiano de Seguridad.

Decreto 1072 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo, Capitulo 6, Art 2.2.4.6.15