PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Diciembre 2024

<table>
<tr><td colspan="2">IDPAC BOGOTÁ</td><td colspan="3">INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL</td></tr>
<tr><td colspan="5">SISTEMA INTEGRADO DE GESTIÓN</td></tr>
<tr><td colspan="5">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>CÓDIGO:</td><td>IDPAC-CENT-PL-02</td><td>VERSIÓN</td><td>04</td></tr>
<tr><td>ELABORÓ</td><td>REVISÓ</td><td colspan="2">APROBÓ</td></tr>
<tr><td>Carlos Iván Porras

Juan Quintero

José Antonio Chaparro

Omar Orlando Coronado</td><td>Yuly Marcela Barjas Aguilar

Edna Piedad Cubillos Caicedo</td><td colspan="2" rowspan="2">Comité Institucional de Gestión y Desempeño</td></tr>
<tr><td>Contratista - Secretaría General

Contratista - Secretaría General

Contratista - Secretaría General

Profesional especializado Código 222-04 – Secretaria General

Contratista - Secretaría General</td><td>Secretaria General

Contratista -Secretaría General</td></tr>
<tr><td>20/12/2024</td><td>23/12/2024</td><td colspan="2">31/12/2024</td></tr>
</table>

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**DESCRIPCIÓN MODIFICACIÓN**
01	26/03/2021	Primer documento aprobado Comité Institucional de Gestión y Desempeño.
02	30/12/2022	Este documento se actualizo en cada uno de sus capítulos enfatizando, el tratamiento de los riesgos sobre los activos de información, el desarrollo del plan plantea desde la identificación el tratamiento y las acciones que llevan al proceso de TI a mitigar los riesgos, de modo que se pueda reaccionar sobre cualquier incidente de seguridad que se presente, evitando que este se materialice.
03	29/12/2023	Este documento se actualiza conforme a lo identificado por el proceso de Comunicación Estratégica y Nuevas Tecnologías-CENT en lo referente al tratamiento y a las acciones que buscan mitigar los riesgos, de tal manera que se gestionen de forma eficiente los incidentes de seguridad que se presenten dando solución a estos.
04	30/11/2024	Armonización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el numeral 6,2 GESTIÓN DE RIESGOS, se agrega el numeral SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.

TABLA DE CONTENIDO

INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información se basa en una orientación estratégica que requiere del desarrollo de una cultura de carácter preventivo, de manera que al comprender el concepto de riesgo, se planteen acciones con el fin de reducir la afectación a la que la Entidad se puede ver expuesta en caso de que llegase a presentarse la materialización de los riesgos identificados.

Adicionalmente, se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos identificados por la entidad con mayor objetividad, con la finalidad de dar a conocer todas aquellas situaciones que pueden llegar a comprometer el cumplimiento de los objetivos trazados por el Instituto en lo referente a los temas de tecnologías de la información.

Conforme a lo expuesto, el IDPAC, tiene implementados atributos de seguridad de acceso para cada uno de los sistemas de información que los funcionarios y contratistas usan diariamente en la ejecución de sus labores. Así mismo la Secretaría General- Tecnologías de la Información, a través del proceso de Gestión de Bienes, Servicios e Infraestructura, administra los sistemas de información y es el responsable de mantener su operatividad los 7 días a la semana, las 24 horas del día.

Ahora bien, la Entidad consiente de los riesgos asociados a las Tecnologías de la Información a los que se ve expuesto, define los objetivos, el alcance, las estrategias, y las acciones necesarias que deben ser divulgadas y aplicadas periódicamente por el personal encargado de la recuperación de los servicios tecnológicos en caso de presentarse la materialización de un riesgo asociado a la pérdida de información.

Finalmente, el Plan de tratamiento de riesgos, busca establecer los lineamientos para la identificación, análisis y monitoreo de los riesgos de seguridad y privacidad de la

información asociados a temas como: perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información. Lo anterior con el propósito de evitar situaciones que afecten el desarrollo de las actividades propias de del Instituto.

1. OBJETIVO

1.1 OBJETIVO GENERAL

Gestionar los riesgos de seguridad de la información, mediante el establecimiento de roles, responsabilidades con el fin de resguardar los servicios y recursos tecnológicos mitigando la afectación a los activos de información en su integridad, confidencialidad y disponibilidad.

1.2 OBJETIVOS ESPECIFICOS

- Involucrar a la Alta Dirección en la gestión proactiva, pertinente y oportuna de los riesgos de seguridad y privacidad de la información.
- Implementar los controles de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los servicios de la entidad.
- Garantizar la continuidad de los servicios tecnológicos como impacto a la continuidad del negocio de la entidad, frente a eventos adversos o catastróficos que sufran causas mayores.
- Reaccionar de forma inmediata ante los eventos fortuitos.
- Apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad del negocio.

2. DOCUMENTOS DE REFERENCIA

- Documento maestro del Modelo de Seguridad y Privacidad de la Información. Versión 4, octubre de 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información. Versión 4, octubre de 2021. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237904_maestro_mspi.pdf

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6, noviembre de 2022.

- IDPAC-PE-GU-01 "*Guía para la Administración del Riesgo del IDPAC*", versión que se encuentre vigente dentro del Sistema Integrado de gestión

3. DEFINICIONES

La tabla de términos y definiciones relacionadas a continuación se extrae de la norma técnica, NTC ISO/IEC 2700, e ISO 27005 vigente, ISO 31000:2018, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

TÉRMINO	DESCRIPCIÓN
Amenaza informática	Posibles ataques lógicos o humanos que puedan interferir con el normal funcionamiento de los equipos de cómputo o con la información que se almacena o procesa en ellos.
Activo de información	Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización, -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.
Amenaza	Peligro latente de que un evento pueda causar un incidente no deseado, presentando daños y/o pérdidas a los activos de información
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Confidencialidad	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Control	Acción o medida que modifica nivel del riesgo
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.

TÉRMINO	DESCRIPCIÓN
Gestión de riesgos	Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos
Información	Es un conjunto organizado de datos, que constituye un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
Integridad	Propiedad de exactitud y completitud.
Impacto	Efecto negativo o positivo que provocaría en caso de que se materializara el riesgo
Nivel de riesgo	Magnitud de un riesgo o de una combinación de riesgos, es la combinación del impacto y posibilidad.
Privacidad	Privacidad: Es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar el tratamiento que se les da a los datos que recolecta o produce.
Probabilidad	se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los

TÉRMINO	DESCRIPCIÓN
	procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo Inherente	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
Riesgo Residual	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riesgo de seguridad y privacidad	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Vulnerabilidad	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. ROLES Y RESPONSABILIDADES

Todas las entidades deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas.

El mayor aporte que genera una definición de roles, es el establecimiento de las tareas que realizará cada uno de los miembros del equipo, evitando que se presenten imprecisiones en referencia a las responsabilidades de cada quien.

Partiendo de este punto, el IDPAC, mediante el esquema de líneas de defensa, define las responsabilidades de cada uno de estos grupos, como se muestra a continuación:

Rol	Responsabilidad
Dirección General – Línea estratégica	• Revisar los cambios en el direccionamiento estratégico del contexto y dar las directrices para evaluar la necesidad de actualizar los documentos de riesgos de la entidad. • Solicitar a los responsables de los procesos la revisión de los riesgos y el seguimiento de las acciones de control. • Revisar los informes emitidos por las unidades de gestión encargadas de la evaluación y control, sobre los resultados de las acciones para el tratamiento de riesgos. • Hacer seguimiento a las acciones de tratamiento de los riesgos para garantizar el cumplimiento de las líneas y que los procesos tomen acciones de mejora continua.
Secretaria General – Tecnologías de la Información – Primera Línea de defensa	• Apropiar documentos al interior del proceso con el fin de determinar actividades de control. • Analizar los riesgos identificados determinando la probabilidad de ocurrencia y consecuencias para establecer el riesgo inherente. • Diseñar y clasificar controles para el tratamiento de riesgos. • Tratar los riesgos definidos mediante implementación de actividades con el fin de reducir su materialización. • Definir acciones de contingencia y aplicarlas en caso de materialización de los riesgos.
Supervisores contractuales – Segunda Línea de defensa	• Hacer seguimiento, evaluación y monitoreo de los riesgos definidos en los procesos durante la ejecución de los contratos hasta la liquidación. • Informar al ordenador del gasto respectivo sobre los resultados del seguimiento a los riesgos durante la ejecución contractual.

Rol	Responsabilidad
Oficina Asesora de Planeación – Segunda línea de defensa	• Establecer contacto para definir lineamientos para la presentación de documentos con estándares de calidad. • Apoyar la actualización los documentos y herramientas de gestión conforme a los avances de tratamiento del riesgo.
Oficina de Control Interno – Tercera línea de defensa	• Realizar el seguimiento periódico al tratamiento de riesgos y a las actividades definidas en el mismo con el fin de generar acciones que evidencien los avances en el tratamiento del riesgo y la mejora continua. • Evaluar de manera objetiva la efectividad del tratamiento y la gestión realizada a los riesgos identificados por la entidad. • Llevar a cabo el seguimiento a los riesgos y la actualización en los documentos de gestión referente al avance en el tratamiento de los mismos. • Revisar la aplicación de los controles e instrumentos de gestión relacionados al tratamiento y la gestión de riesgos.

5. NORMATIVIDAD

La normatividad relacionada a continuación es la sugerida para su consulta en las guías de elaboración de documentos obligados en el marco del cumplimiento de MSPI, por el Ministerio de las Tecnologías de la Información

- Ley 1273 de 2009: "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado, "de la protección de la información y*

de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Ley 1581 de 2012: "*Por la cual se dictan disposiciones generales para la protección de datos personales*"

- Ley 1712 de 2014: *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*

- CONPES 3854 de 2016: *Política de Seguridad Digital del Estado Colombiano*
- CONPES 3995 de 2020: *Política Nacional De Confianza y Seguridad Digital*
- Decreto 1078 de 2015: *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
- Decreto 1499 de 2017: Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión
- Decreto 612 de 4 de abril de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

6. DESCRIPCIÓN

6.1 PLAN DE TRATAMIENTO Y MITIGACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD.

EL IDPAC busca crear una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del proceso de Comunicación Estratégica y Nuevas Tecnologías - CENT, identificando y gestionando los riesgos de los procesos y proyectos que aportan a la

lucha contra la corrupción, mediante la implementación de mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo los controles para lograr la eficiencia a lo largo del ciclo de vida del proyecto, aportando a la optimización de forma oportuna para responder a los riesgos de seguridad y privacidad de la Información y Seguridad de manera Integral.

Como entidad debemos estar preparados para prevenir todo tipo de ataques o desastres, puesto que al materializarse el riesgo, el costo de recuperación supera al costo de prevención, lo que hace que la implementación de planes de gestión de riesgos, permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

La metodología para la identificación, evaluación y gestión de riesgos se basa en la NTC-ISO 31000, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP , principalmente en lo dispuesto en su Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones, y finalmente en lo establecido en la Guía para la Administración del Riesgo del IDPAC, la cual se basa en los documentos mencionados y esto permite la mejora continua y el cumplimiento de los objetivos institucionales mediante el establecimiento de los controles que aportan al fortalecimiento y la mejora en el desempeño de los procesos y la transparencia en la gestión Institucional.

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información.
- La criticidad de los activos de información involucrados.

- Los requisitos legales y reglamentarios, así como las obligaciones contractuales de los contratos que suscriba la entidad.
- La importancia de la disponibilidad, integridad y confidencialidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la entidad.

Por lo anterior y en atención al esquema de líneas de defensa definido en la entidad, se realiza la gestión de los riesgos para el proceso de Comunicación Estratégica y Nuevas Tecnologías del IDPAC. Para ello, las actividades de identificación y análisis de los riesgos se realizan con los líderes de cada proceso como propietarios de los activos de información, por lo cual deben garantizar que los custodios de la información cumplan con los controles establecidos para procurar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional.

6.2 GESTIÓN DE RIESGOS

A fin de determinar las falencias del Instituto, en lo referente a la gestión del riesgo, se deben identificar, analizar y monitorear los controles de estos, con el propósito de proporcionar un aseguramiento razonable respecto del alcance de los objetivos del IDPAC. En este sentido se definen las siguientes actividades.

Actividad	Responsables	Meta	Unidad de medida de la meta	Programado trimestral			
				Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
Revisión de Inventario activos de información Tipo Software, Hardware y Servicios IDEP. Con el fin de realizar la actualización.	Funcionarios o Contratistas Gestión de Tecnologías de la información	IDPAC-CENT-PR-03 Actualización de Inventario de Activos de Información V4	Instrumento Actualizado y revisado	0	0	1	0
Apoyar la identificación del inventario con los Activos de información del IDEP.	Funcionarios o Contratistas Gestión de Tecnologías de la información	Gestión con las diferentes áreas del IDPAC según la necesidad	Actas de reuniones	1	1	0	0
Publicar el Registro de AI del Área de Tecnología en el portal web del IDPAC.	Funcionarios o Contratistas Gestión de Tecnologías de la información.	1 Registro de AI de Tecnología	Registro de AI publicado	0	0	0	1
Capacitación y formación para incluir aspectos relacionados con seguridad de la	Funcionarios o Contratistas Gestión de Tecnologías de la información	4 capacitación	Presentaciones, fotos, listas de asistencias	1	1	1	1

Actividad	Responsables	Meta	Unidad de medida de la meta	Programado trimestral			
				Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
información, activos de información a los funcionarios del IDPAC.							
Divulgar y gestionar los boletines informativos de seguridad, generado por las diferentes entidades o por el IDPAC.	Funcionarios o Contratistas Gestión de Tecnologías de la información	100 % de los boletines remitidos al oficial de seguridad del IDPAC.	Boletines Informativos Divulgados	1	1	1	1
Definición e implementación de configuraciones desde la consola del antivirus, generando reportes de seguimiento	Funcionarios o Contratistas Gestión de Tecnologías de la información	3 informes de gestión	Reportes de informe con acciones técnicas realizadas	1	1	1	1
Definición e implementación de configuraciones desde la	Funcionarios o Contratistas Gestión	3 informes de gestión	Reportes de informe con acciones	1	1	1	1

Actividad	Responsables	Meta	Unidad de medida de la meta	Programado trimestral			
				Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
consola del firewall, generando	de Tecnologías de la información		técnicas realizadas				
Parametrización de la gestión de cambio de contraseñas en los usuarios de domino y aplicaciones del IDEP	Funcionarios o Contratistas Gestión de Tecnologías de la información	Configuración el servidor de dominio y aplicaciones	Reportes de informe con acciones técnicas realizadas	1	1	1	1
Gestionar el proceso de Backup, garantizando la restauración de copias de respaldo a aplicaciones y sistemas	Funcionarios o Contratistas Gestión de Tecnologías de la información	BackUps de servidores y aplicaciones.	Informe de gestión	1	1	1	1
Actualizar las actividades del plan de tratamiento de riesgos de seguridad y privacidad de la información – IDAPC para la	Contratistas Oficina Asesora de Planeación. Técnico Oficina Planeación	IDPAC-CENT-PL-02 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la	Plan actualizado y publicado en la SIGPARTICIPO	0	0	0	1

Actividad	Responsables	Meta	Unidad de medida de la meta	Programado trimestral			
				Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
siguiente vigencia.		Información Vx					

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información así mismo, teniendo en cuenta la criticidad de los activos de información, la cual fue valorada de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MinTIC[1], una buena práctica consiste en realizar gestión de riesgos a estos activos que se consideren con nivel de clasificación ALTA dependiendo de la calificación que se realice, según los criterios de clasificación (confidencialidad, Integridad y Disponibilidad) como se muestra continuación:

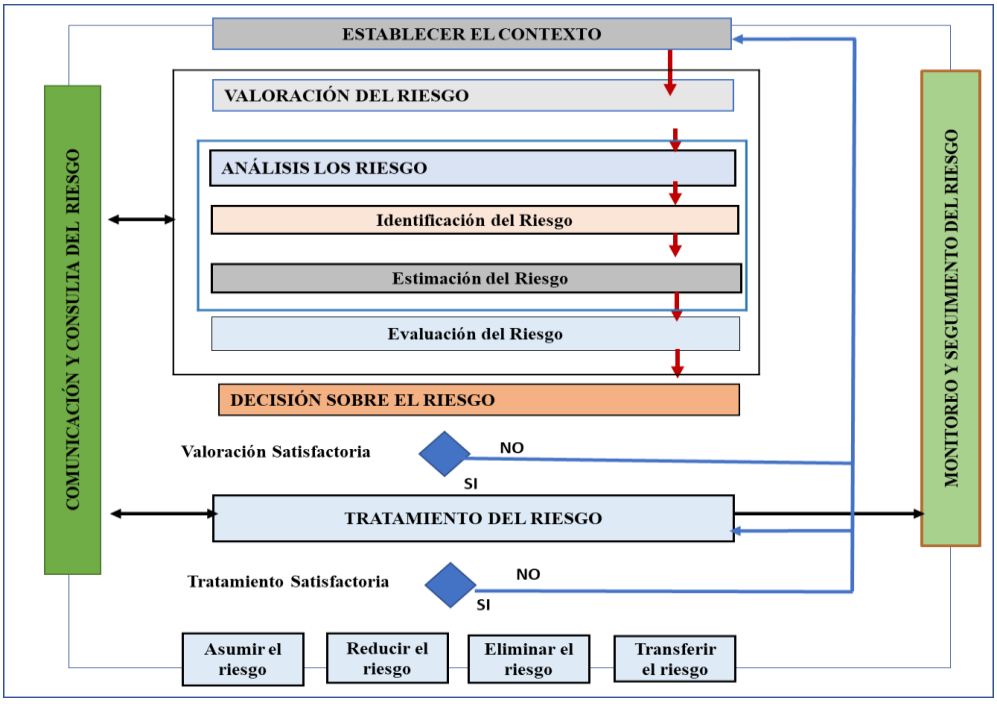
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA(M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA(B)	BAJA (3)
INFORMACIÓN NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

[1] Guía para la 0020 de Activos de Información de MinTIC, referenciada en el Anexo 4

El proceso identificación y gestión de riesgo en la seguridad de la información pretende definir el enfoque organizacional para la valoración del riesgo, su tratamiento y posterior control de este.

6.3 CICLO DE LA GESTIÓN DE RIESGOS

El modelo de gestión de riesgos de seguridad de la información diseñado y basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en seguridad de la información; los elementos que lo componen son:



Fuente: Tomado de la norma ISO/IEC 27005 Proceso para la administración del riesgo

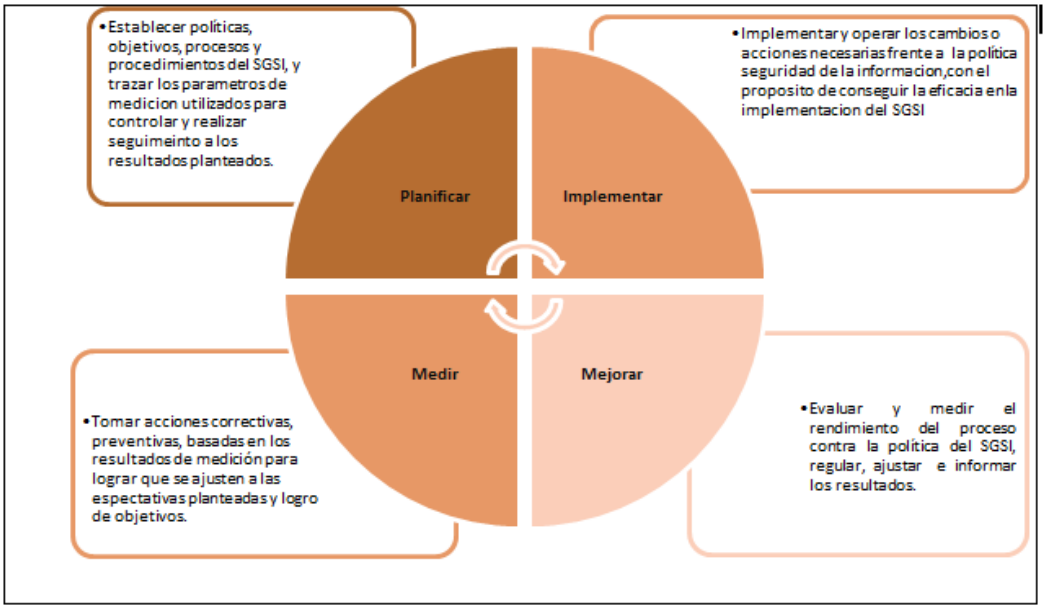
6.4 COMUNICACIÓN Y CONSULTA

El Proceso de Comunicación Estratégica y Nuevas Tecnologías, para mantener una buena comunicación con las partes interesadas, grupos de valor y ciudadanía en general dispone de los diferentes canales de comunicación de la entidad con el fin de garantizar que se comprendan las bases sobre las cuales se toman decisiones.

6.5 ESTABLECIMIENTO DE CONTEXTO

Para la definición del contexto estratégico, se tiene en cuenta lo definido en el Plan Estratégico Institucional, por lo tanto, el diseño de esta primera etapa se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales y asociados a la seguridad y privacidad de la información.

Igualmente, se debe tener en cuenta el objetivo del proceso “Comunicación Estratégica y Nuevas Tecnologías”, el cual se encuentra documentado en la caracterización, como una herramienta en la identificación de los factores internos y externos que influyen sobre la gestión del riesgo, para lo que se utilizará el ciclo de mejora continua PHVA que toma como punto de partida en la identificación de riesgos, la clasificación de activos de información de los procesos.



6.6 VALORACIÓN DEL RIESGO

La valoración de riesgos de seguridad de la información toma como insumo la identificación del inventario de activos de información de los procesos, el cual es la base del enfoque de la valoración de los riesgos de seguridad de la información, consiste en valorar la probabilidad y el impacto del riesgo analizado, con el fin de determinar el nivel del riesgo inherente.

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la cual se retoma a continuación:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

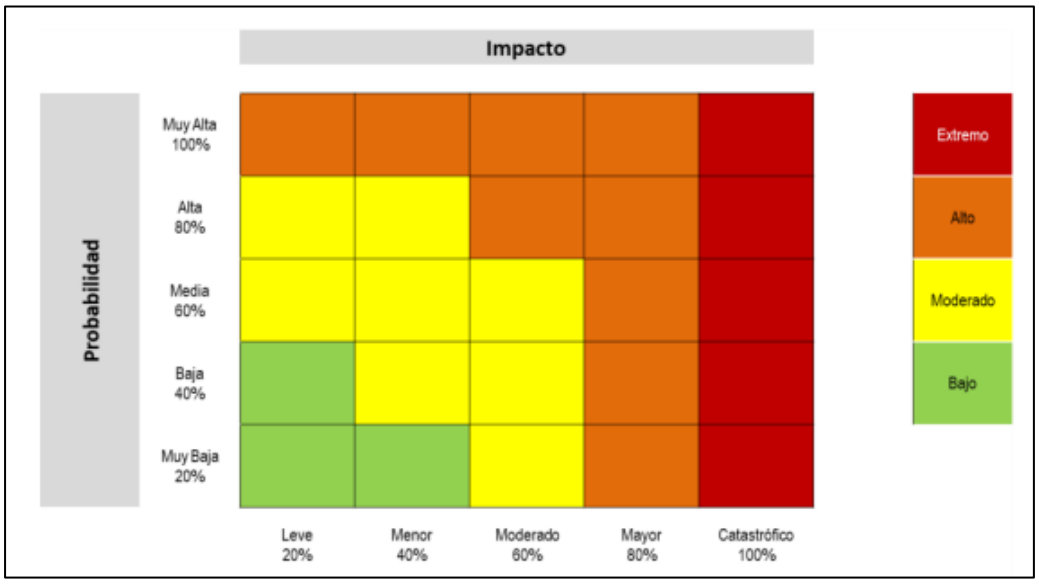
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6, noviembre de 2022

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo. En este sentido, se debe considerar para este análisis la tabla que se retoma a continuación:

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6, noviembre de 2022

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



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6, noviembre de 2022

6.7 ANALISIS DE RIESGOS

El propósito es comprender la naturaleza del riesgo y sus características incluyendo el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y

puede afectar a múltiples objetivos. Este paso tiene como fin establecer la probabilidad de ocurrencia y el nivel de impacto, con el fin de estimar el nivel del riesgo inherente.

6.8 IDENTIFICACIÓN DEL RIESGO

El proceso de Comunicación Estratégica y Nuevas Tecnologías, podrá identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Es importante mencionar que para cada uno de los riesgos se deben relacionar los activos específicos del proceso, y a su vez realizar un análisis de las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Es importante mencionar que para que una vulnerabilidad cause daño, se requiere que exista una amenaza que ataque la debilidad identificada. Si se identifican vulnerabilidades que no tienen amenazas es probable que no se requiera implementar un control.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Escucha encubierta
Red	Líneas de comunicación sin protección	Escucha encubierta

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

6.9 ESTIMACIÓN O ANÁLISIS DE LOS RIESGOS

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- **Evitar**: Es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir**: Planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad.
- **Reducir o mitigar**: Corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia

planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.

- **Dispersar**: Es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad.
- **Compartir:** Es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad.

6.10 EVALUACIÓN DE LOS RIESGOS

La Norma ISO 31000 estable que la evaluación de la gestión del riesgo debe realizarse con base en los resultados del análisis de riesgos. La finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar. La evaluación del riesgo es la comparación de los niveles de riesgo estimados con los criterios de evaluación y los criterios de aceptación del riesgo.

6.11 EVALUAR LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS EN EL IDPAC

La evaluación de los controles se debe realizar cuando se ha establecido el riesgo inherente para los procesos, junto con el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos.

La evaluación de controles en el IDPAC se debe llevar a cabo identificando los criterios relacionados a cada uno de los riesgos establecidos ya descritos. Para ello se establecen las características que permiten establecer un seguimiento y verificación de los controles establecidos:

- **Naturaleza del control**: se debe definir cómo se va a llevar a cabo el control, si este control se hace manual, automático o ambos.
- **Documentación:** es necesario que todo el control se documente y se lleva un seguimiento de las actualizaciones y nuevos eventos.
- **Evidencias**: Revisión de la documentación, periodicidad, divulgación y demás actividades registradas que requieran para llevar a cabo la retroalimentación, las acciones de mejora y el control.
- **Tipo de control**: el IDPAC debe tener como prioridad el control investigativo, luego el preventivo y por último el correctivo y dejar documentación de estos en caso de que se presenten o puedan ser detectados a tiempo y cuál fue el proceso de mitigación.

6.12 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo es establecido por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Ahora bien, al momento de evaluar las opciones existentes para el tratamiento del riesgo, es importante iniciar con lo establecido en la política de administración del riesgo del Instituto. Con dicha información los responsables de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Si se presenta el caso en el que al responder ante un riesgo se genere un riesgo residual que supere los niveles aceptables, será necesario volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.

Partiendo de base del resultado del análisis de riesgo con el fin de tratar el riesgo residual se deben establecer los niveles de riesgo y se adelantan acciones de mejora que propenden por conservar las características de confidencialidad, integridad y disponibilidad de la información.

NIVELES DE RIESGO			
TIPO DE RIESGO	**VALOR ASIGNADO**	**GESTIÓN**	**ACTIVIDADES O TAREAS**
Riesgo Catastrófico	Si su ocurrencia es mayor a doce (12) veces en un año o se presenta varias veces en un (1) mes.	MITIGAR	Requiere acciones inmediatas para evitar la pérdida de la confidencialidad, integridad y disponibilidad de la información. Documentar.
Riesgo Alto	Si su ocurrencia es mayor a ocho (8) veces en un año, pero menor a diez (10) o se presenta al menos una vez en dos meses consecutivos.	MITIGAR	Se requiere de acciones rápidas que contempla la toma de decisiones conjuntas entre la alta dirección y tecnología del IDPAC. Documentar.
Riesgo Moderado	Si su ocurrencia es mayor a cinco (5) veces en un año, pero menor a ocho (8) o se presenta al menos una vez en dos meses no consecutivos para ese periodo.	MITIGAR	Se requiere revisar y ejecutar los controles establecidos para el riesgo y revisar eficacia de estos. Documentar.
Riesgo Bajo	Si su ocurrencia es mayor a dos (2) veces en un	ACEPTAR	El riesgo se mitiga con actividades propias, controles

NIVELES DE RIESGO			
TIPO DE RIESGO	**VALOR ASIGNADO**	**GESTIÓN**	**ACTIVIDADES O TAREAS**
	año, pero menor a cinco (5) o se presenta al menos una vez en un mes para ese periodo.		establecidos y por medio de acciones de investigación y preventivas.
Riesgo insignificante	Si ocurre una (1) vez en el año	ACEPTAR	El riesgo no representa impacto significativo para el IDPAC.

Las opciones de tratamiento de riesgos según ISO 31000:2018 no son excluyentes entre sí y tampoco resultan eficaces en todas las circunstancias, éstas pueden incluir una o varias de las siguientes acciones:

- Asumir el riesgo, aun aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para reducir el riesgo la probabilidad del riesgo.
- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Transferir el riesgo o compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros)
- Retener el riesgo con base en información confiable.

6.13 MONITOREO Y REVISIÓN

Como parte del proceso de gestión del riesgo, los riesgos y los controles deberían ser monitoreados y revisados regularmente para comprobar que:

- La hipótesis acerca de los riesgos sigue siendo válida.
- La hipótesis en la que está basada la valoración del riesgo, incluyendo el contexto interior y exterior, sigue siendo válida.
- Se van cumpliendo los resultados esperados.
- La técnica de valoración del riesgo se aplica correctamente.
- Los tratamientos del riesgo son efectivos.

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios que exijan la valoración reiterada de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad, por lo tanto podrán cambiar de forma o manera radical sin previo aviso.

Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos de información.
- Nuevas amenazas.
- Cambios o aparición de nuevas vulnerabilidades.
- Aumento de las consecuencias o impactos.
- Incidentes de seguridad de la información.

Con el fin de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y

medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

6.14 ACTIVIDADES

Las actividades que se relacionan a continuación se realizarán conforme a los documentos para el tratamiento de los riesgos que hacen parte del sistema integrado de gestión de la entidad en el marco de los lineamientos del Modelo Integrado de Planeación y Gestión - MIPG.

6.14.1 IDENTIFICACIÓN DE AMENAZAS

Eventos que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos, pueden desencadenar o explotar una vulnerabilidad para comprometer algún aspecto del activo del listado de amenazas y vulnerabilidades en ISO 27001

- Acceso a la red o al sistema de información por personas no autorizadas.
- Amenaza o ataque con bomba.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Comprometer información confidencial.
- Ocultar la identidad de un usuario.
- Daño causado por un tercero.
- Daños resultantes de las pruebas de penetración.
- Destrucción de registros.
- Desastre generado por causas humanas.
- Desastre natural, incendio, inundación, rayo.
- Revelación de información.

- Divulgación de contraseñas.
- Malversación y fraude.
- Errores en mantenimiento.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Espionaje industrial.
- Fuga de información.
- Interrupción de procesos de negocio.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.
- Mal funcionamiento del equipo.
- Código malicioso.
- Uso indebido de los sistemas de información.
- Uso indebido de las herramientas de auditoría.
- Contaminación.
- Errores de software.
- Huelgas o paros.
- Ataques terroristas.
- Hurtos o vandalismo.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Instalación no autorizada de software.
- Acceso físico no autorizado.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.
- Error de usuario.

6.14.2 IDENTIFICACIÓN DE VULNERABILIDADES

Las vulnerabilidades se refieren a los defectos o debilidades en un activo, conforme al listado de vulnerabilidades en ISO 27001

- Interfaz de usuario complicada.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.
- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.

- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.
- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.
- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.

Las amenazas y vulnerabilidades contempladas en ISO 27001 deben ser correctamente identificadas y constituyen un aspecto clave del sistema de seguridad y privacidad de la información del IDPAC. Las vulnerabilidades en ISO 27001 van de la mano y, por esa razón, se deben considerar en su conjunto.

6.14.3 TRATAMIENTO Y ACEPTACIÓN

El equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

Propende que la entidad elabore un instrumento de medición y resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados.

Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de estos y la prioridad de implementación de cada proyecto.

7. METODOLOGÍA PROPUESTA LA IDENTIFICACIÓN TRATAMIENTO Y MITIGACIÓN DE LOS RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos propone de manera inmersa las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC: 2016):

7.1 DESARROLLO METODOLÓGICO

Etapa 1: Análisis de la información, se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar la política de tratamiento de riesgos
- Establecer los controles (se desprenden de las medidas definidas por la entidad)
- Precisar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

Etapa 2: Desarrollo del proyecto, se realizarán las actividades que permitan la estructuración de las medidas de valoración del riesgo:

- Establecer el nombre de la medida a realizar
- Concretar los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Obtener la justificación de la medida.
- Concretar las actividades a realizar para el desarrollo de la medida.

Etapa 3: Análisis de los proyectos

- Sentar controles relacionados con cada medida.
- Admitir los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.

Etapa 4: Definición del organigrama de responsabilidad, se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Caracterización de las funciones materia de seguridad de la información.
- Segunda línea de defensa: Esta línea está conformada por la Oficina Asesora de Planeación, quien responde de manera directa por el aseguramiento de la operación; su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. Así mismo, consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para

evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión".

- Asignación de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

7.2 RECURSOS REQUERIDOS

En la inferencia de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se debe disponer de los siguientes recursos:

- **Humanos**: El proceso de Comunicación Estratégica y Nuevas Tecnologías a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento y aplicación de políticas lo concerniente a la seguridad y privacidad de la información, contribuye a la mejora continua.
- **Financieros**: Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y mejora de auditorías.
- **Técnicos**: Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI).
- **Logísticos**: Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

7.3 ACTIVIDADES QUE EJECUTAR

Las actividades a realizar a corto, mediano y largo plazo se definen de forma anual en el Plan de Acción Institucional , con el fin de gestionar los riesgos y de esta manera, desplegar mecanismos de tratamiento de riesgo e instrumentos para la mitigación de los riesgos identificados evaluados y valorados, mediante el desarrollo de cada una de

las actividades consignadas en este documento, con el fin de dejar registrado un informe cuatrimestral de los riesgos por los cuales pasaron los diferentes activos de información del IDPAC.

8. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El IDPAC “evaluará el plan de tratamiento de riegos de seguridad y privacidad de la información”, por medio de un monitoreo esencial para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables del proceso de Gestión de Tecnologías de la información, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

9. ANEXOS

- Plan de Acción Institucional formulado para cada vigencia