ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE GOBIERNO
Departamento Administrativo de la Defensoría del Espacio Público

Procedimiento ASEGURAR LA OPTIMIZACIÓN DEL RIESGO

Proceso GESTIÓN DE LA INFORMACIÓN Y LA TECNOLOGÍA

VIGENCIA: **15/09/2020** | CODIGO: **127-PRCGI-EMD03-01** | **V1**

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	15/09/2020	N.A

OBJETIVO

Asegurar que el apetito y la tolerancia al riesgo de la entidad son entendidos, articulados y comunicados y que el riesgo relacionado con el uso de las TI es identificado y gestionado.

ALCANCE

Incia examinando y evaluando continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la entidad, continua con la orientación de la implantación de prácticas de gestión de riesgos para propocionar una seguridad razonable y supervisa los objetivos y métricas clave de la gestión del riesgo.

DEFINICIONES Y SIGLAS

APETITO DE RIESGO:es el nivel de riesgo que la empresa quiere aceptar.
TOLERANCIA AL RIESGO: es la desviación respecto al nivel de riesgo.
CAPACIDAD: es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.

POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

1. Las actividades que son punto de control, serán señaladas dentro del Flujograma con la figura de cuadrado y la sigla P.C dentro de ella.
2. Cuando en las actividades se presenten incumplimiento de requisitos de norma o de los clientes y/o usuarios, deberán implementarse el procedimiento denominado "Acciones correctivas, preventivas y de mejora".
3. Cuando dentro del procedimiento se incluyan acciones de divulgación o comunicación estas deberán realizarse en el marco del Plan de comunicaciones del Departamento y deberá tener en cuenta los procedimientos y protocolos establecidos.

PRODUCTO O SERVICIO

SALIDAS (Producto o Servicio)	DESCRIPCIÓN	GRUPOS DE VALOR OBJETIVO
Guías del apetito del riesgo Niveles de tolerancia del riesgo aprobados Evaluación de las actividades de gestión de riesgo Políticas de gestión de riesgo Objetivos a ser monitoriados por la gestión de riesgos Proceso aprobado para la medición de la gestión de riesgo Acciones correctivas a tratar las desviaciones de la gestión del riesgo	Aseguramiento de la optimización del riesgo	Comité Directivo Usuarios internos

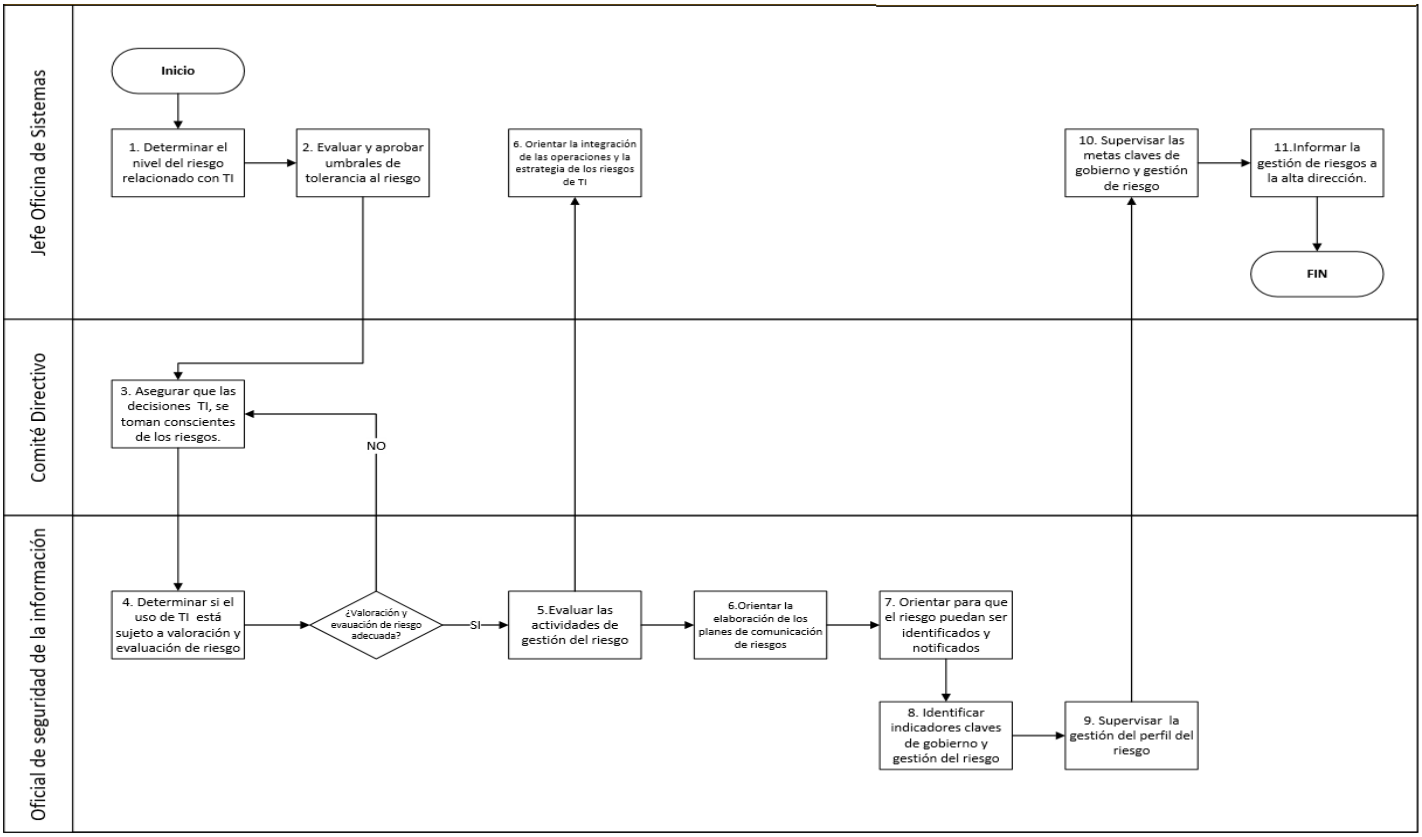
NORMATIVIDAD Y/O DOCUMENTOS ASOCIADOS

- El control de los riesgos a la seguridad de la información, riesgos laborales, aspectos ambientales se pueden consultar el el siguiente vinculo: Mapa de Riesgos.
- La normativa asociada al procedimiento se puede consultar en el siguiente vinculo: Matriz de requisitos legales y normativos
- Los documentos asociados al procedimiento se pueden consultar en el siguiente vinculo: Listado Maestro de Documentos.
- Los registros asociados al procedimiento se pueden consultar en el siguiente vinculo: Listado Maestro de registros/ Cuadro de Caracterización Documental
- Las disposiciones de almacenamiento y archivo se pueden consultar en el siguiente vinculo: Tablas de Retención Documental.
- Entradas y salidas,RACI, metricas relacionadas al procedimiento.

ACTIVIDAD	FLUJOGRAMA	DESCRIPCIÓN ACTIVIDAD	TIEMPO	RESPONSABLE	FORMATO Y/O REGISTRO
	Ver Anexo EMD03-Flujograma	INICIO			
1		Determinar el nivel del riesgo relacionado con TI que la entidad esta dispuesta a asumir para cumplir con los objetivos.	3 días	Jefe Oficina de Sistemas	Nivel riesgo
2		Evaluar y aprobar umbrales de tolerancia al riesgo frente a los niveles de riesgo aceptables por la entidad	3 días	Jefe Oficina de Sistemas	Umbrales de toleracia del riesgo de TI
3		Asegurar que las decisiones de la entidad en terminos tecnológicos, se toman conscientes de los riesgos.	5 días	Comité Directivo	
4		Determinar si el uso de TI está sujeto a valoración y evaluación de riesgo adecuada de acuerdo a la normatividad establecida. ¿Valoración y evauación de riesgo adecuada? Si: continuar con la activiada 5. No: regresar a la actividad 3	2 días	Oficial de seguridad de la información	
5		Evaluar las actividades de gestión del riesgo para garantizar su alineación a las capacidades de la entidad en las perdidas de TI.	5 días	Oficial de seguridad de la información	Mapa de riesgos TI
6		Orientar la elaboración de los planes de comunicación de riesgos	2 días	Oficial de seguridad de la información	
7		Orientar para que los riesgos puedan ser identificados y notificados por cualquier persona en cualquier momento.	2 días	oficial de seguridad de la información	
8		Identificar indicadores claves de gobierno y gestión del riesgo para ser monitoreados y aprobar métodos y técnicas para recolectar y notificar la información de medición	2 días	oficial de seguridad de la información	indicadores de riesgo
9		Supervisar la gestión del perfil del riesgo dentro de los umbrales del apetito de riesgo	2 días	Oficial de seguridad de la información	
10		Supervisar las metas claves de gobierno y gestión de riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas.	2 días	Jefe Oficina de Sistemas	Mapa de riesgos TI
11		Informar la gestión de riesgos a la alta dirección.	1día	Jefe Oficina de Sistemas	Mapa de riesgos TI
		FIN.			

AUTORIZACIÓN

Elaboró:	Revisó:	Aprobó:
Guiomar Cortés Ávila Gerente de Proyectos OS	Luis Fernando Arango Vargas Profesional Universitario Oficina Asesora de Planeación	Claudia Liliana Paipa Jefe Oficina de Sistemas


Jefe Oficina de Sistemas
Comité Directivo
Oficial de seguridad de la información
Inicio
1. Determinar el nivel del riesgo relacionado con TI
2. Evaluar y aprobar umbrales de tolerancia al riesgo
6. Orientar la integración de las operaciones y la estrategia de los riesgos de TI
10. Supervisar las metas claves de gobierno y gestión de riesgo
11.Informar la gestión de riesgos a la alta dirección.
FIN
3. Asegurar que las decisiones TI, se toman conscientes de los riesgos.
NO
4. Determinar si el uso de TI está sujeto a valoración y evaluación de riesgo
¿Valoración y evauación de riesgo adecuada?
SI
5.Evaluar las actividades de gestión del riesgo
6.Orientar la elaboración de los planes de comunicación de riesgos
7. Orientar para que el riesgo puedan ser identificados y notificados
8. Identificar indicadores claves de gobierno y gestión del riesgo
9. Supervisar la gestión del perfil del riesgo