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

ESE
HOSPITAL DEL SUR
ITAGÜÍ

Contenido

INTRODUCCIÓN

La información que de genera al interior de las entidades públicas, se convierte en un activo fundamental, ya que se utiliza como insumo para la toma de decisiones, mejorar la relación con los usuarios y orientar los objetivos estratégicos. Lo anterior implica, que se hace necesario realizar un inventario y clasificación de los Activos de Información, ya que éste es la base para la gestión de riesgos de seguridad y privacidad de la información y así determinar los niveles de protección requeridos.

La institución en el desarrollo diario de su misión sustenta a través de las TIC, los procesos de captura, procesamiento y reporte de información tanto al interior de la entidad como al exterior para comunicarse con otros actores del sistema de salud, lo que implica que la institución sea vulnerable a eventos que comprometan la integridad, disponibilidad y seguridad de la Información.

De acuerdo a lo mencionado anteriormente, La **ESE Hospital del Sur** "**Gabriel Jaramillo Piedrahita**" acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar con la finalidad de minimizar pérdidas, maximizar rendimientos y sobre todo teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Definir una metodología que permita el tratamiento de los riesgos relacionados con la seguridad y privacidad de la información asociados a la operación de la **ESE Hospital del Sur "G.J.P."** y que puedan afectar el cumplimiento de los objetivos estratégicos.

1.2. OBJETIVOS ESPECIFICOS

- ✓ Realizar un diagnóstico de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información.
- ✓ Fomentar el uso y apropiación de la Política de Seguridad de la información en los funcionarios de la ESE Hospital del Sur "G.J.P."
- ✓ Involucrar y comprometer a la alta dirección y a los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

2. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución que intervengan en la captura, almacenamiento, procesamiento y reporte de información Institucional.

3. DEFINICIONES

- ✓ **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- ✓ **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- ✓ **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- ✓ **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- ✓ **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- ✓ **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española). Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- ✓ **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- ✓ **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- ✓ **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- ✓ **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- ✓ **Riesgo:** 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).

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

- ✓ **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar

dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- ✓ **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- ✓ **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- ✓ **Amenaza**: situación externa que no controla la entidad y que puede afectar su operación

4. MARCO LEGAL

- ✓ **Decreto 1008 de 2018** - Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- ✓ **Decreto 612 de 2018** - Por el cual se fijan directrices para a Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- ✓ **Resolución 3564 de 2015** - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

- ✓ **Decreto 1078 de 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- ✓ **Ley 1712 de 2014** - Ley de Transparencia y acceso a la información pública.

- ✓ **Decreto 2609 de 2012** - Por el cual se reglamenta el Título V de la Ley 594 de 2000.

- ✓ **Ley Estatutaria 1581 de 2012** - Protección de datos personales.

- ✓ **Ley 594 de 2000** - Ley General de Archivos.

- ✓ **Ley 527 de 1999** - Ley de Comercio Electrónico.

5. DESCRIPCIÓN DEL PLAN

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía N° 7 Gestión de riesgos y la Guía N° 8 Controles de seguridad de la información del Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC.

En la siguiente imagen se muestra el procedimiento de la Guía N° 7 que propone el Departamento administrativo de la función pública (DAFP) en concordancia con el Ministerio de Tecnologías de la información y comunicaciones (MinTIC) para la gestión de riesgos de Seguridad de Información.

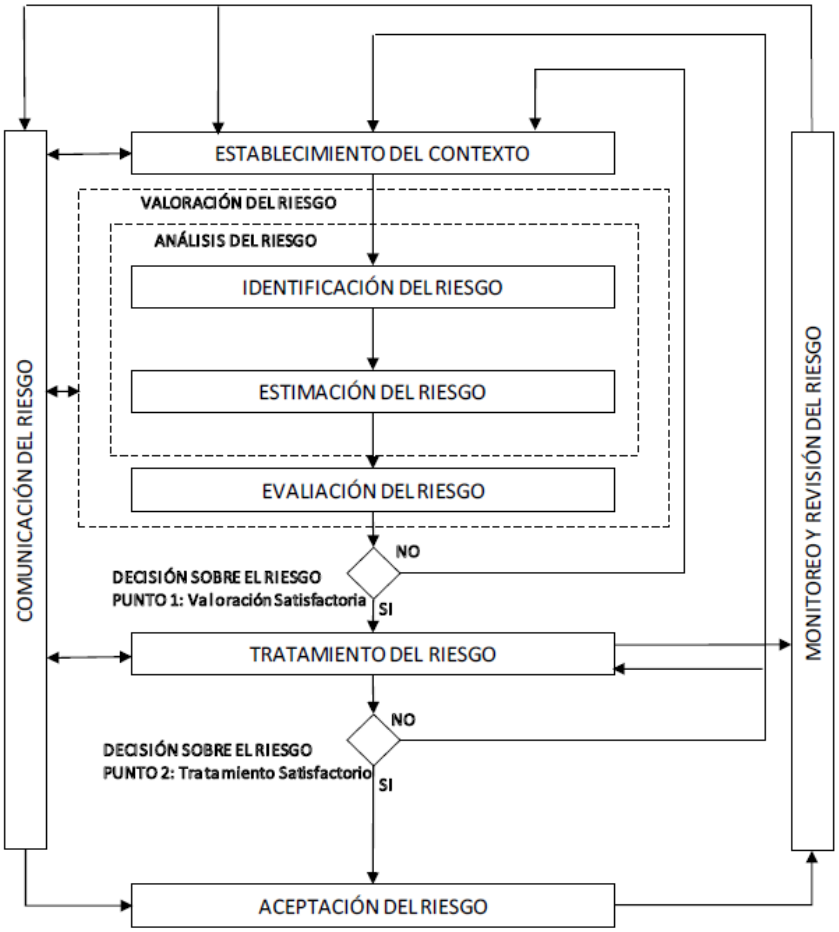


Imagen 2. Tomado de la NTC-ISO/IEC 27005

5.1. ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO

Definir el contexto marca la ruta que la entidad debe seguir frente a la exposición al riesgo, ya que permite conocer las situaciones que pueden afectar el cumplimiento de los objetivos en este caso los criterios de seguridad y privacidad de la información, se analizan los activos de información desde la estructura organizacional, los recursos físicos y tecnológicos, entre otros.

Para establecer el contexto para la gestión del riesgo es necesario definir los criterios de riesgo de seguridad y privacidad de la información:

CRITERIOS DE EVALUACIÓN DEL RIESGO:

Para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización se tienen en cuenta los siguientes aspectos.

- ✓ El valor estratégico del proceso evaluado.
- ✓ Criticidad de los activos de información.
- ✓ Los requisitos legales, reglamentarios y contractuales.
- ✓ Valoración de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.

CRITERIOS DE IMPACTO

Los criterios de impacto del riesgo se especifican en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad y privacidad de la información, considerando los siguientes aspectos:

- ✓ Nivel de clasificación de los activos de información del proceso
- ✓ Brechas en la seguridad dela información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- ✓ Operaciones deterioradas.
- ✓ Perdida del negocio y del valor financiero.
- ✓ Alteración de planes y fechas límites.
- ✓ Daños para la reputación.
- ✓ Incumplimiento de requisitos legales.

CRITERIOS DE ACEPTACIÓN DEL RIESGO

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- ✓ Criterios del negocio
- ✓ Aspectos legales y reglamentarios
- ✓ Operaciones
- ✓ Tecnología
- ✓ Finanzas
- ✓ Factores sociales y humanitarios

La **ESE Hospital del Sur "G.J.P."** define los siguientes criterios para la aceptación del Riesgo.

- ✓ Si al realizar la evaluación de los controles, la diferencia entre el riesgo inherente y el residual es tolerable o aceptable, el riesgo no necesitaría ser tratado. Pero se debe continuar con la aplicación de los controles definidos y el monitoreo permanente del comportamiento del riesgo.

- ✓ Para realizar el cálculo del riesgo residual, será necesario evaluar la efectividad de los controles.

- ✓ Cuando el impacto de la materialización del riesgo residual sea mayor o catastrófico, los Líderes de los procesos deberán establecer planes de contingencia que permitan proteger la institución en caso de su ocurrencia.

- ✓ Si existen procesos en los cuales, se tienen identificados riesgos y no poseen controles, se deben implementar para evitar la materialización de los mismos.

Tabla de Ejemplo.

N° Riesgo	Descripción del Riesgo	Tipo de Riesgo	Causas		Consecuencias
			Internas	Externas	
RISK02	Accesos no autorizados a infraestructura tecnológica (servidores, bases de datos, estaciones de trabajo, redes y servicios de red).	Seguridad y Privacidad de la Información	Contraseñas fáciles de Identificar. Obsolescencia tecnológica. Falta de equipo se seguridad perimetral.	Accesos no autorizados	Perdida de la confidencialidad, integridad, y disponibilidad de la información.

5.2. VALORACIÓN DEL RIESGO

Para la identificación y evaluación se toma como base el contexto de la entidad donde se analiza el origen de las situaciones de riesgo ya sea en el ámbito interno o externo.

A partir de los factores internos y externos, se determinan los agentes generadores del riesgo de seguridad y privacidad de la información sus causas y sus consecuencias: pérdida, daño, perjuicio o detrimento.

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.

IDENTIFICACION 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.

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.

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.

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.

IDENTIFICACIÓN DE LAS CONSECUENCIAS

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras

Para la identificación de las consecuencias es necesario tener:

- ✓ Lista de activos de información y su relación con cada proceso de la entidad.
- ✓ Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

5.3. ANALISIS DEL RIESGO

Para realizar el análisis se utiliza las siguientes tablas para evaluar la probabilidad y el impacto:

Criterios para clasificar la probabilidad de ocurrencia del riesgo

Probabilidad	
Raro (1)	La Probabilidad de Ocurrencia es muy baja, casi Nula.
Improbable (2)	Puede ocurrir bajo circunstancias Excepcionales.
Posible (3)	Puede ocurrir con cierta frecuencia.
Probable (4)	Ocurre algunas veces.
Casi seguro (5)	Se espera que el evento ocurra en la mayoría de las circunstancias.

Criterios para la calificación del impacto del riesgo

Impacto	
Insignificante (1)	La materialización de los riesgos, no afecta a ningún proceso.
Menor (2)	La materialización de los riesgos, afecta levemente al Hospital.
Moderado (3)	Las consecuencias de la materialización de los riesgos pueden afectar parcialmente los procesos y servicios del Hospital, pero las pérdidas y daños son menores y no afectan la imagen institucional.
Mayor (4)	Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios del Hospital y afectarse la imagen institucional.
Catastrófico (5)	Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación de la Entidad.

5.4. EVALUACIÓN DEL RIESGO

Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos.

Además, permite ver las zonas de riesgo presentando las posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

Matriz de Calificación, Evaluación y respuesta a los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

5.5. TRATAMIENTO DE RIESGO

La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

Zona de Riesgo	Tratamiento
Zona de Riesgo Baja (B)	Asumir el riesgo.
Zona de Riesgo Moderada (M)	Asumir el riesgo, Reducir el riesgo.
Zona de Riesgo Alta (A)	Reducir el Riesgo, Evitar, compartir o Transferir.
Zona de Riesgo Extrema (E)	Reducir el Riesgo, Evitar, compartir o Transferir.

En esta etapa se describen los controles o barreras a ser implementadas o fortalecer las ya existentes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto.

Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones comparativas, fortalecer la plataforma tecnológica existente, Sensibilización de los usuarios internos, asesoría de expertos, entre otras.

5.6 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS

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

Los riesgos son dinámicos por tanto podrán cambiar de forma o manera inesperada. Por ello es necesario una supervisión continua para identificar: Nuevos activos o modificaciones en nivel de criticidad, Nuevas amenazas,

nuevas vulnerabilidades, Aumento de las consecuencias o impactos e incidentes de seguridad de la información.

Con el propósito 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.

La Entidad definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad y privacidad de la información en todos sus procesos, basado con su criticidad y su valor para el cumplimiento de su misión.

PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

Las oficinas de control interno y la subdirección administrativa , coordinarán si es necesario la actualización de la política de administración de riesgos y las fechas de corte para el registro y monitoreo.

ESCANEO DE VULNERABILIDADES

Programar y realizar el escaneo de vulnerabilidades sobre el total de los servicios de información, el cual se realizará con una herramienta comercial y con la última versión disponible. La calificación de las vulnerabilidades se realiza a través del Common Vulnerabilities and Exposure - CVE; en los casos cuando la vulnerabilidad no se encuentra en CVE, pero ha sido confirmada por el fabricante, la clasificación se realizará directamente por la herramienta de escaneo de vulnerabilidades. El insumo para la mitigación de vulnerabilidades es el reporte de la herramienta, la cual indica la descripción y posible solución.

MITIGACIÓN DE VULNERABILIDADES

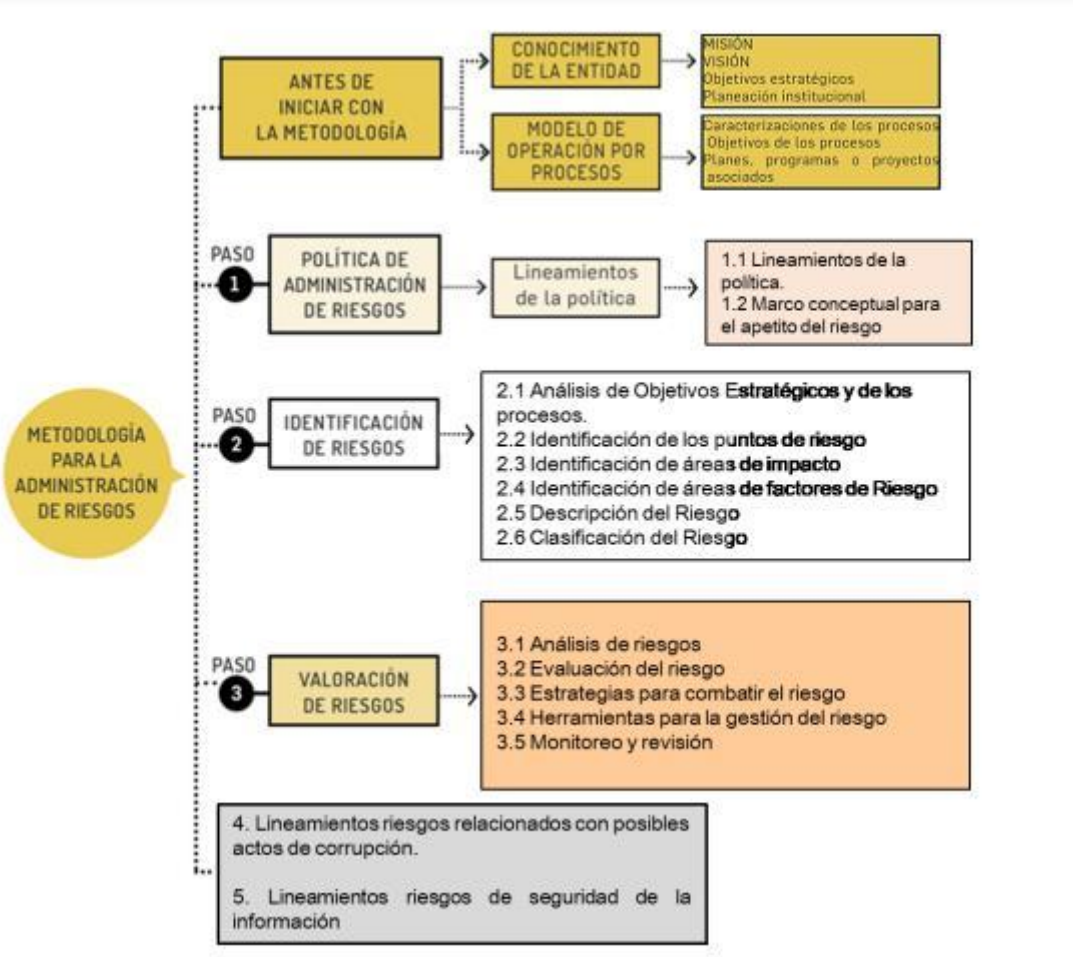
Basado en el reporte del escaneo de vulnerabilidades se prioriza el accionar iniciando con las vulnerabilidades de riesgo crítico y alto. En caso de no poder realizar una mitigación, se validarán controles o medidas necesarias para evitar la explotación de estas.

SOCIALIZACIÓN DEL ESTADO ACTUAL DE LOS SERVICIOS DE INFORMACIÓN

Socializar con los lideres y enlaces de activos de información el estado tecnológico de cada uno de los servicios de información de los cuales sean propietarios, con el fin de llevar a cabo planes de mejora o adquisición tecnológica según corresponda**.**

CAPACITACIÓN SOBRE RIESGOS DE SEGURIDAD

Realizar capacitación a los enlaces definidos por los directivos de área para que puedan realizar la identificación de riesgos de seguridad digital, orientada bajo la siguiente metodología:



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

Identificar los riesgos de seguridad digital basados en la capacitación realizada. Durante este proceso la Oficina de Gestión de la informacion realizará los acompañamientos que se requieran a los enlaces, teniendo en cuenta que cada área tiene el conocimiento claro y preciso de su proceso y pueden identificar la forma en que la confidencialidad, integridad y disponibilidad, se pueden ver afectadas.

CREACIÓN DE PLANES DE TRATAMIENTO

Crear planes de tratamiento cuando el riesgo residual quede en valores no aceptables por la entidad de acuerdo con la guía de tratamiento del riesgo y sea necesario reducirlo.

CARGUE DE RIESGOS EN EL SIG

Cargar en el Sistema Integrado de Gestión los riesgos identificados para los activos de información con los respectivos controles actuales y los planes de mejoramiento que se llevarán a cabo.

AJUSTAR MAPA DE RIESGOS

Validar los riesgos que se cargaron y de esta manera ajustar el mapa de riesgos con la información entregada por cada área.

SEGUIMIENTO A LOS CONTROLES Y PLANES DE MEJORAMIENTO

Realizar seguimiento a la información cargada por parte de cada área con respecto a los controles y planes de mejora para cada trimestre del año.

6. REFERENCIAS

- ✓ **Modelo de Seguridad y Privacidad de la Información – MSPI**, Ministerio de Tecnologías de la Información y las Comunicaciones.

- ✓ **Guía N° 7 - Gestión de riegos**. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones.

- ✓ **Guía N° 8 - Controles de seguridad y privacidad de la información**. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones.

7. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	31/Ene/2019	Se crea el Plan de Tratamiento de riesgos de seguridad y privacidad de la información, como parte de la Estrategia Gobierno Digital del MinTIC.
2	31/01/2024	Actualización del plan adición de nuevo capitulo

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Responsable Gerencia de la Información	**Nombre:**	Líder de Calidad.	**Nombre:**	Freddy Leon Valencia Arroyave
Cargo:	Profesional Universitario Ingeniero de Sistemas	**Cargo:**	Líder de Calidad.	**Cargo:**	Gerente
Fecha:	31/Ene/2024	**Fecha:**	31/Ene/2024	**Fecha:**	31/Ene/2024