Salud Sogamoso E.S.E.

TABLA DE CONTENIDO

HISTORIA 2
TABLA DE CONTENIDO 3
1. DERECHOS DE AUTOR 4
2. AUDIENCIA 5
3. INTRODUCCIÓN 6
4. OBJETIVOS DE LA GUÍA 8
5. ETAPAS SUGERIDAS PARA LA GESTIÓN DEL RIESGO 9
6. VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN 10
7. CONTEXTO ESTRATÉGICO 13
8. CRITERIOS BASICOS 14
8.1. CRITERIOS DE EVALUACIÓN DEL RIESGO 14
8.2. CRITERIOS DE IMPACTO 14
8.3. CRITERIOS DE ACEPTACIÓN DEL RIESGO 15
9. ALCANDE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION 16
10. IDENTIFICACIÓN DE RIESGOS 17
11. ANÁLISIS DE RIESGOS 19
11.1. IDENTIFICACIÓN DEL RIESGO 19
11.2. IDENTIFICACIÓN DE LOS ACTIVOS 19
11.3. IDENTIFICACIÓN DE LAS AMENAZAS 19
11.4. IDENTIFICACIÓN DE CONTROLES EXISTENTES 22
11.5. IDENTIFICACIÓN DE LAS VULNERABILIDADES 23
11.6. MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS 30
11.7. IDENTIFICACIÓN DE LAS CONSECUENCIAS 30
12. EVALUACIÓN DE RIESGO 31
12.1. EVALUACIÓN DEL RIESGO 32
13. VALORACIÓN DE CONTROLES PARA EL TRATAMIENTO DE RIESGOS. 34
14. PLAN DE IMPLEMENTACIÓN 36
15. POLÍTICAS DE ADMINISTRACIÓN DEL RIESGO 39

La información que hace parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte Teniendo en cuenta que el contexto organizacional de esta guía y del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa la presente guía es la "Guía de Riesgos" del DAFP [1] , buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de éste modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

Es así como alineando los Objetivos estratégicos de la Entidad, al desarrollo del MSPI se logra una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión por ejemplo el MECI[2].

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:

[1] Departamento de la Función Pública - DAFP
[2] Modelo estándar de Control Interno.

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

Tabla 1. 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 2. Niveles de Clasificación

4. OBJETIVOS DE LA GUÍA

A través de ésta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.

Ayudar a que las Entidades logren vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.

5. ETAPAS SUGERIDAS PARA LA GESTIÓN DEL RIESGO

De acuerdo con lo señalado en la Guía de Gestión del Riesgo del DAFP (en adelante, la guía), se tienen tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la Entidad tener una administración de riesgos acorde con las necesidades de la misma.

De esta forma la primera y más importante para lograr un adecuado avance en todo el proceso de administración del riesgo es el "Compromiso de las alta y media dirección" puesto que al igual que como se menciona en la guía, tener el verdadero compromiso de los directivos garantizan en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona en el MSPI la necesidad de tener aprobación de la dirección en cada etapa es necesaria.

Así mismo en concordancia con lo estipulado en la guía "debe designar a un directivo de primer nivel (debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del MECI y el Sistema de Gestión de la Calidad) que asesore y apoye todo el proceso de diseño e implementación del

Componente"[3], el MSPI se acoge puesto que lo que se busca es lograr una gestión integral del riesgo.

En segundo lugar se encuentra la "Conformación de un Equipo MECI o de un grupo interdisciplinario", la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la Entidad y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis para el MECI, o para el modelo de Gestión de Calidad.

Finalmente se encuentra la "Capacitación en la metodología", este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI, para tener un contexto Organizacional en todos los aspectos del desarrollo del MSPI.

[3] Tomado de la Guía Gestión de Riesgo del DAFP, Las etapas sugeridas para una adecuada administración del Riesgo.

6. VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo:

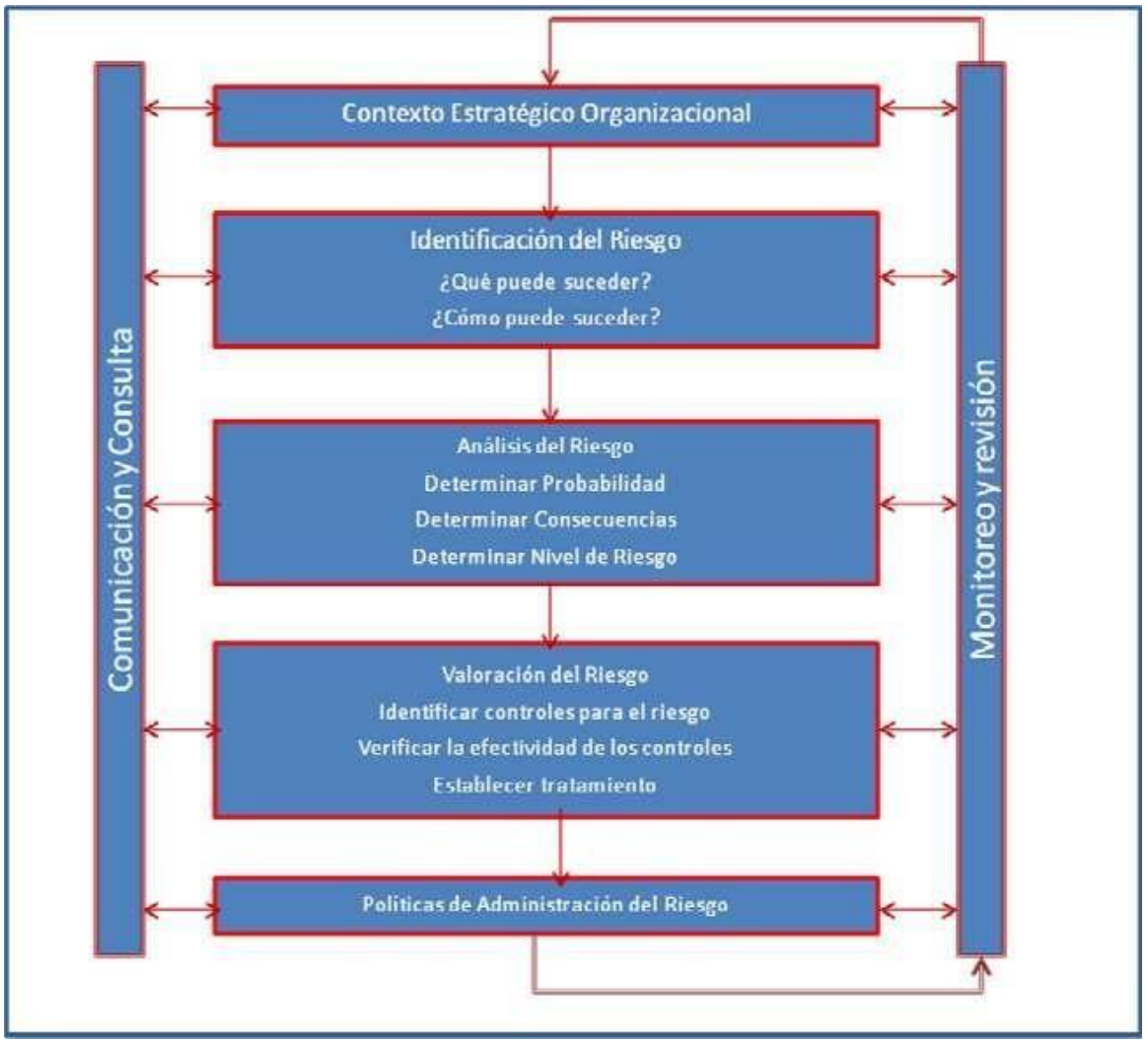


Imagen 1. Tomado de la Cartilla de Administración de Riesgos del DAFP

- Proceso para la administración del riesgo en seguridad de la información

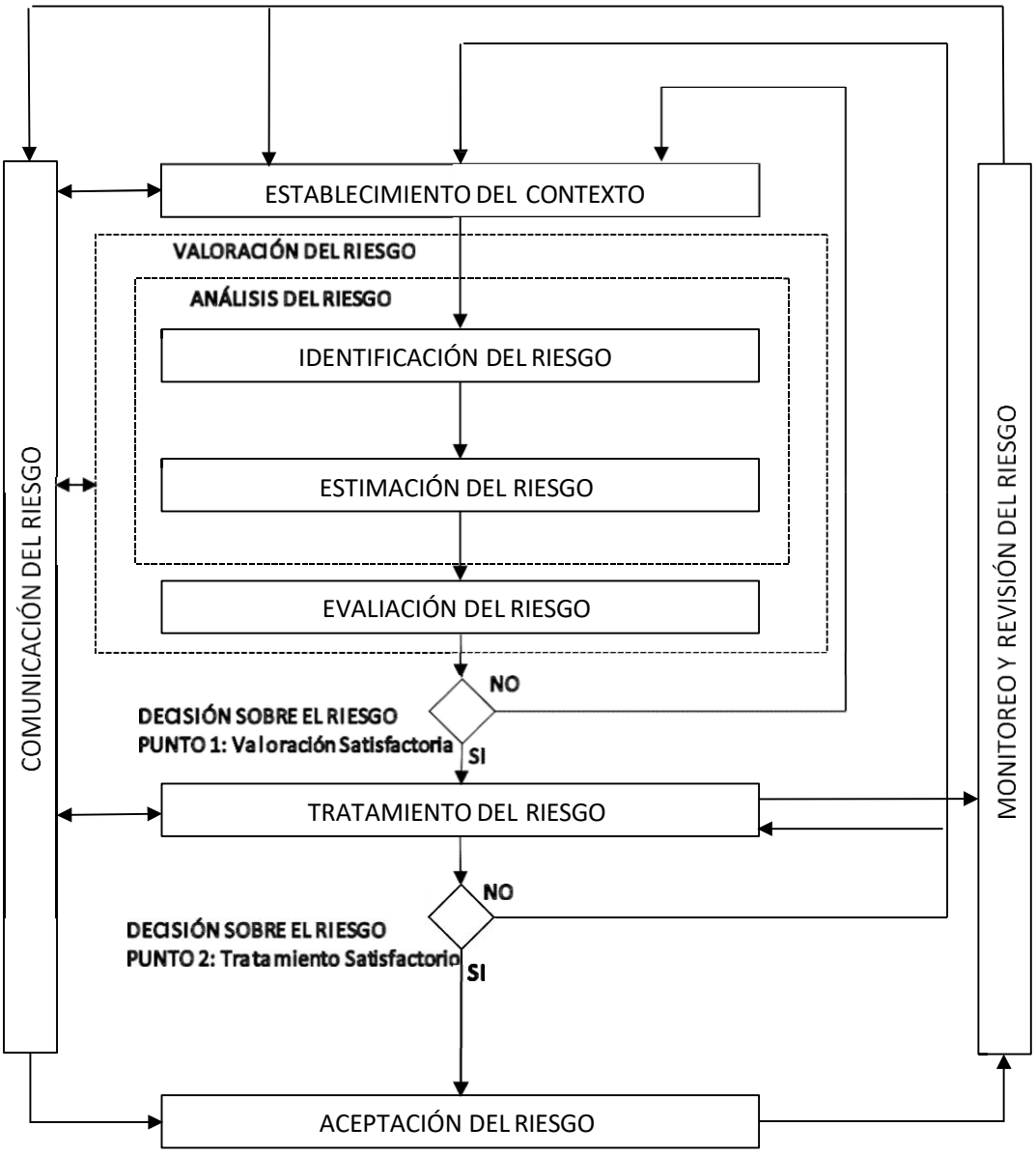


Imagen 2. Tomado de la NTC-ISO/IEC 27005

Así como lo ilustra la imagen 2 el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevara a cabo otra iteración de la valoración del riego con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo criterios para la valoración del riesgo, de aceptación o de impacto del riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 3. Etapas de la Gestión del Riesgo a lo Largo del MSPI

7. CONTEXTO ESTRATÉGICO

El contexto estratégico se tiene en cuenta en el proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la Entidad, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la Entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI.

Sin embargo cabe mencionar que la guía señala las siguientes estrategias a través de las cuales se puede hacer ese levantamiento del contexto Estratégico[4] :

1. ***Inventario de Eventos***
2. ***Talleres de Trabajo***
3. ***Análisis de Flujo de Procesos***

Es esencial determinar el propósito de la gestión del riego en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un BCP.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- El resultado de la especificación del contexto estratégico es la especificación de los criterio básicos alcance, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

[4] La descripción específica de éstas se encuentra en la Guía de Riesgo del DAFP, páginas 18 y 19 - ¿qué es Contexto Estratégico?

8. CRITERIOS BASICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

8.1. CRITERIOS DE EVALUACIÓN DEL RIESGO:

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

De igual modo, los criterios de evaluación de impacto del riesgo y se pueden utilizar para especificar las prioridades del tratamiento del riesgo.

8.2. CRITERIOS DE IMPACTO.

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información del procesos
- 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 limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

8.3. CRITERIOS DE ACEPTACIÓN DEL RIESGO

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar las siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

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

9. ALCANCE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Es importante que la entidad defina el alcance y los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

Al definir el alcance y los límites la entidad debería considerar la siguiente información

- Objetivos estratégicos de negocio, políticas y estrategias de la organización
- Procesos del negocio
- Funciones y estructura de la organización
- Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- La política de seguridad de la información de la organización
- El enfoque global de la organización hacia la gestión del riesgo
- Activos de información
- Ubicación de la organización y sus características geográficas
- Restricciones que afectan a la organización
- Expectativas de las partes interesadas
- Entorno sociocultural
- Interfaces (Ej. Intercambio de información con otras entidades)

10. IDENTIFICACIÓN DE RIESGOS

De acuerdo a lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

En este momento es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con éste punto se revisa la pertinencia del alcance planteado para el MSPI.

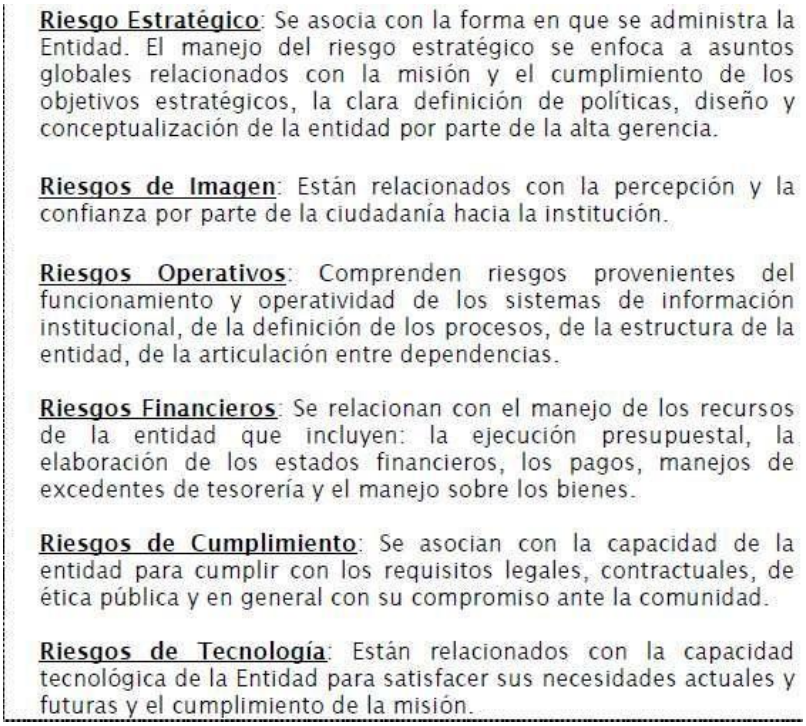
En esta etapa es especialmente importante la participación del personal designado para la implementación del MSPI, dentro de la mesa interdisciplinaria en la cual se revisan los procesos, tomando parte en la identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.

Para este capítulo, la guía inicia con la definición de algunos términos que son necesarios dentro del empleo de ésta metodología, estos términos son comúnmente empleados en las Entidades ara efectos de la aplicación del sistema de Calidad o el MECI, y se listarán a continuación:

- Proceso.
- Objetivo del Proceso.
- Identificación de Activos.
- Riesgo.
- Causas (Amenazas y Vulnerabilidades).
- Descripción del Riesgo.
- Efectos de la materialización del Riesgo.

Como acto seguido se debe realizar la clasificación de los riesgos, para esto *la guía* presenta las siguientes opciones:

Ilustración 1 lista de Clasificación de Riesgos



Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico 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.

Fuente: Guía de Riesgos DAFP

La entidad tiene la posibilidad de agregar a este listado los riesgos de seguridad que considere pertinentes dentro del desarrollo del MSPI en el proceso de identificación del riesgo, teniendo en cuenta cómo se podría vulnerar alguno de los pilares de la seguridad de la información:

- Disponibilidad
- Confidencialidad
- Integridad

11. ANÁLISIS DE RIESGOS

Para la entidad es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí la Entidad tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la Entidad decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual la entidad sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI.

A continuación se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005.

11.1. 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.

11.2. 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*.**

11.3. 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, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	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	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
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 2: Amenazas Comunes

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
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	- Bomba/Terrorismo - Guerra de la información - Ataques contra el sistema DDoS - Penetración en el sistema - Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos	Ventaja competitiva Espionaje económico	- Ventaja de defensa - Ventaja política - Explotación económica

extranjeros, otros intereses)		• 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.

11.4. 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.

11.5. 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
	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 o documentos
	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
	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)	
ORGANIZACIÓN	Ausencia de 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 auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de	Abuso de los derechos

	administradores y operadores	
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso

	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo

	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

11.6. MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS:

TIPOS DE PRUEBAS DE EFECTIVIDAD

Pueden realizarse 3 tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o infraestructura de la entidad objetivo:

- **Pruebas Con Conocimiento Nulo Del Entorno:** Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco o nulo conocimiento del objetivo o su infraestructura.
- **Pruebas Con Conocimiento Medio Del Entorno:** Es cuando para la prueba de pentesting, se tiene más información sobre el ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc… pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.
- **Pruebas Con Conocimiento Completo Del Entorno:** Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.

11.7. IDENTIFICACIÓN DE LAS CONSECUENCIAS

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.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

En esta actividad se deben identificar los daños o las consecuencias para entidad que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

Las entidades deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

12. EVALUACIÓN DE RIESGO

Para continuar con el análisis y la evaluación del riesgo depende de la información obtenida en las fases de identificación anteriormente descritas de Identificación de los riesgos, es por ello que la entidad debe crear los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización.

De esta forma *la guía* menciona cuales son los pasos claves en el análisis de riesgos, probabilidad e impacto, definiendo como sigue cada uno de ellos[5]:

"Por Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo".

De esta forma se procede a hacer la "calificación del riesgo", en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

De igual forma *la guía* presenta una "tabla de probabilidad" y una "Tabla de Impacto", en las cuales presenta 5 niveles para medir la probabilidad de ocurrencia y 5 niveles para lograr medir el impacto, dando las herramientas con las cuales se definen los criterios de riesgo.

Por otro lado presenta la tabla en la cual se señalan "los impactos de mayor ocurrencia en las Entidades del Estado"[6], en éste punto se toca el impacto sobre la Confidencialidad de la Información, el cual es uno de los pilares de la Seguridad de la Información.

[5] Guía de Riesgos DAFP, pág 24.
[6] Guía de Riesgos DAFP.

Ilustración 2 Impacto Sobre la Confidencialidad de la Información

NIVEL	CONCEPTO
1	Personal
2	Grupo de Trabajo
3	Relativa al Proceso
4	Institucional
5	Estratégica

Fuente: Guía de Riesgos DAFP

Este puede ser el punto de partida para la inclusión de los temas de seguridad de la Información dentro del análisis hecho para los procesos que se cubrirán según el alcance del MSPI, así pues podría extenderse el análisis hacia la Integridad y la Disponibilidad de la Información.

12.1. 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”, con la cual *la guía* presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

Ilustración 3 “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

13. VALORACIÓN DE CONTROLES PARA EL TRATAMIENTO DE RIESGOS

Esta etapa se debe tener en cuenta la evaluación realizada en el numeral 10.4 inicia con la evaluación de los controles existentes en la Entidad, estableciendo su descripción, su formalidad (¿se aplican?, ¿están documentados?) y su efectividad (calificación en la matriz de riesgos) para luego ser comparados con los criterios definidos en las etapas de identificación y análisis de riesgos, de esta forma se busca escoger los controles que permitan disminuir los valores de exposición del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad; en la definición de éstos nuevos controles, se utiliza la tabla de "estructura de controles" que presenta la guía de controles del MSPI, para hacer un trabajo documentado y Ordenado.

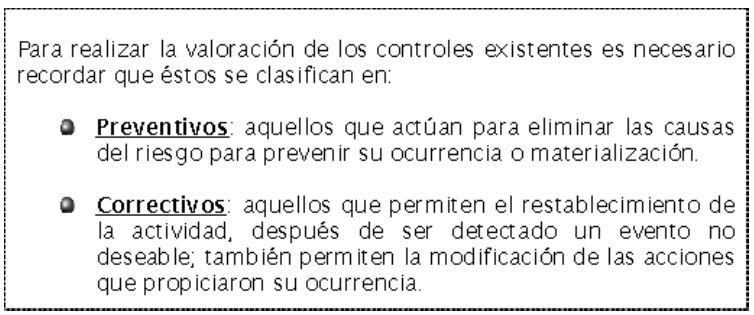
Tabla 2 – Estructura de controles

Política general			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
	…		

Fuente: Guía – Controles del MSPI

Por otro lado, para hacer una clasificación y valoración de los controles, se debe tener en cuenta que en *la guía*, se presenta una clasificación entre dos tipos de Controles, Preventivos y Correctivos definidos como se indica en la siguiente ilustración:

Ilustración 5 – Tipos de Controles



Fuente: Guía de Riesgos del DAFP

Por otro lado, *la guía* facilita las siguientes herramientas con las cuales se logra hacer una cuantificación del análisis de los controles elegidos.

Ilustración 6. Tablas para valoración de controles

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Fuente: guía de Riesgos del DAFP

14. PLAN DE IMPLEMENTACIÓN

Luego de elegir cuáles controles son los más adecuados para tener un nivel de riesgo aceptable para el o los procesos incluidos en el alcance del MSPI, se debe diseñar un plan de tratamiento de riesgos incluyendo los de Seguridad de la información, en el cual se defina qué tratamiento se dará a los riesgos de acuerdo con las opciones entregadas en la guía[7], qué acciones se implementarán, quienes serán los responsables de ésta implementación. Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución del mismo.

Teniendo en cuenta que se debe tener la aprobación del plan de tratamiento de riesgos por parte de los dueños de cada riesgo, que en este caso y como se ha venido planteando, corresponderían a los dueños de los procesos, es indispensable que la aceptación del plan de tratamiento de riesgos y del riesgo residual se haga en el comité interdisciplinario designado para estos temas en la Entidad y así se logra dar la participación de las diferentes áreas incluidas en el proceso y finalmente de la Dirección.

Tabla 3 - Valoración del riesgo

VALORACIÓN DEL RIESGO							
PROCESO: ATENCIÓN AL USUARIO							
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.							
RIESGO	**CALIFICACIÓN**		**CONTROLES**	**VALORACIÓN**			
	Probabilidad	**Impacto**		**Tipo Controles Prob. o Impacto**	**PUNTAJE Herramientas para ejercer el control**	**PUNTAJE Seguimiento al control**	**Puntaje Final**
Cambio en los datos de contacto de los usuarios	3	4	Procedimientos establecidos para la asignación de Roles y Perfiles dentro del sistema	PROBABILIDAD	35	20	55

[7] Opciones de tratamiento del riesgo, Guía de Riesgos DAFP, pág 33.

			Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema, generando alarmas ante anomalías	PROBABILIDAD	30	25	55

De acuerdo con el análisis anterior, ya el riesgo se podría reducir dos puntos en Probabilidad, de acuerdo a las calificaciones de los controles, como se muestra en la siguiente ilustración:

Ilustración 7. Revisión de Controles

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 Riegos DAFP, adecuación Autor

Tabla 4 - Nueva Valoración de Acuerdo a Los Controles Identificados

ANÁLISIS DEL RIESGO					
PROCESO: ATENCIÓN AL USUARIO					
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.					
RIESGO	**CALIFICACIÓN**		**Tipo Impacto**	**Evaluación**	**Medidas de Respuesta**
	Probabilidad	**Impacto**		**Zona de Riesgo**	

Cambio en los datos de contacto de los usuarios	1	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	ALTA	Reducir el Riesgo Evitar Compartir o Transferir

De toda la información recolectada anteriormente se obtiene el Mapa de riesgos en el cual se presenta un resumen de las acciones empleadas para la identificación, análisis y evaluación de riesgos, así como de la evaluación y elección de los controles, tal como se presenta en el siguiente cuadro que entrega *la guía*:

Tabla 5- Mapa de riesgos

MAPA DE RIESGOS											
PROCESO: ATENCIÓN AL USUARIO											
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.											
RIESGO	**CALIFICACIÓN**		**Evaluación**	**CONTROLES**	**NUEVA CALIFICACIÓN**		**Evaluación**	**Medidas de Respuesta**	**ACCIONES**	**RESPONSABLE**	**INDICADOR**
	Prob	**Impa**	**Zona de Riesgo**		**Prob**	**Imp**	**Zona de Riesgo**				
Cambio en los datos de contacto de los usuarios	3	4	EXTREMA	Procedimientos establecidos para la asignación de Roles y Perfiles dentro del sistema	3	4	ALTA	Reducir el Riesgo Evitar Compartir o Transferir	Capacitación al nuevo personal que asigna usuarios sobre el sistema.	Áreas responsables del manejo del sistema - Área de tecnología	Nuevo personal vinculado VS Usuarios formados y conocedores de los procedimientos.
				Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema					Inclusión de alarmas ante anomalías.		Número de solicitudes de usuario vs Cantidad de alarmas sobre el sistema

15. POLÍTICAS DE ADMINISTRACIÓN DEL RIESGO

Las políticas de administración del riesgo estarán guiadas por el trabajo realizado anteriormente, complementando los resultados y procedimientos del MSPI, sobre todo para los temas de la definición de la declaración de aplicabilidad (SOA), el cual es el documento con las justificaciones de la aplicación o elección de los controles, en éste también se justifica porque no se eligieron los controles que hayan quedado por fuera, después del plan de tratamiento de riesgos.

Finalmente, no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados.

Agregar lo de almera ciclo PHVA riesgos