VIGILADA MINEDUCACIÓN

PROFESIONAL LFA Ruta de la calidad

Capacitamos para la Transformación Productiva

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PTRSPI)

2022-2025

Por

MARIO GERMÁN CALDAS MARTÍNEZ

X

GUSTAVO ADOLFO RUBIO LOZANO
Rector

CLAUDIA XIMENA TRIANA VERA
Vicerrector Académico

DARÍO ALFONSO PAYÁN SANCLEMENTE
Asesor

Guadalajara de Buga, Valle del Cauca
2023

Tabla de contenido

Lista de tablas.

Lista Ilustraciones

Abreviaturas y acrónimos

Abreviatura	Significado
AAC	Acreditación de Alta Calidad
AE	Arquitectura Empresarial
AI	Arquitectura de Información
AMP	Acuerdo Marco de Precios
ANS	Acuerdos de Niveles de Servicio
ATI	Arquitectura de la Tecnología de la Información
BCP	Plan de Continuidad del Negocio - Business Continuity Plan
BPM	Business Process Model and Notation (Notación y modelamiento de procesos de negocios)
CIO	Chief Information Officer - Líderes de la gestión estratégica de Tecnologías de Información (TI), encargados de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI, y todo lo de esta tarea
CMMI	Integración de modelos de madurez de capacidades - Capability Maturity Model Integration
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas - Control Objectives for Information and related Technology
CONPES	Consejo Nacional de Política Económica y Social
CT+I	Ciencia, Tecnología e Innovación
DAFP	Departamento Administrativo de la Función Pública
DNP	Departamento Nacional de Planeación
EPCA	Encuesta de Percepción Ciudadana sobre Calidad y Accesibilidad de Trámites y Servicios
ESP	Programa de Estrategia Empresarial (Enterprise Strategy Program)

GTIC	Grupo de Tecnologías de la información y las Comunicaciones
I+D	Investigación y Desarrollo
IGC	Índice Global de Competitividad
INC	Informe Nacional de Competitividad
IT4+	Modelo de Gestión Estratégica de Tecnologías de la Información
ITA	Instituto Técnico Agrícola
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información - Information Technology Infraestructure Library
MECI	Modelo estándar de Control Interno
MGPTI	Modelo de Gestión de Proyectos
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
MIPG	Modelo Integrado de Planeación y Gestión
MRAE	Marco de Referencia de Arquitectura Empresarial
MSPI	Modelo de Seguridad y Privacidad de la Información
NOC	Network Operations Center, Centro de Operaciones de Redes
OCDE	Organización para la Cooperación y el Desarrollo Económico
PEI	Plan Estratégico de Tecnologías de la Información
PETI	Plan Estratégico de las Tecnologías de Información y las Comunicaciones
PMBOK	Guía de los Fundamentos de Gestión de Proyectos - Guide to the Project Management Body of Knowledge, es un libro de estándares, pautas y normas para la gestión de proyectos.
PMI	Project Management Institute
PMO	Oficina de Gestión de Proyectos - Project Management Office
PND	Plan Nacional de Desarrollo
PQRS	Peticiones, Quejas, Reclamos y Solicitudes.
PSI	Plan de Seguridad de la Información
RGC	Reporte Global de Competitividad
RPO	Punto de Recuperación Objetivo - Recovery Point Objective
RTO	Tiempo de Recuperación Objetivo - Recovery TIme Objective
SGSI	Sistema de Gestión de la Seguridad de la Información
SOC	Centro de Operación de Seguridad - Security Operation Center
TI	Tecnologías de la Información
TIC	Tecnología de la Información y las Comunicaciones

Definiciones

Término	Definición
Actividades	Acciones a desarrollar en una institución de manera cotidiana, como parte de sus obligaciones, tareas o funciones.
Activo de Información	En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
Administración del riesgo	Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Amenaza	Es la causa potencial de una situación de incidente y no deseada por la organización
Análisis de Riesgos	Es el uso sistemático de la información disponible para determinar la frecuencia para determinados eventos donde se pueden producir y la magnitud de sus consecuencias.
Aplicaciones	Es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas
Arquitectura	Según ISO/IEC 42010: Proceso de concebir, expresar, documentar, comunicar, certificar la implementación, mantener y mejorar la arquitectura a través de todo el ciclo de vida de un sistema
Arquitectura de TI	Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
Arquitectura Empresarial	Es una práctica estratégica (una capacidad), consiste en analizar integralmente las empresas desde diferentes perspectivas o dimensiones (el negocio, la información, las aplicaciones, la infraestructura), con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria.
Arquitectura Misional o de Negocio	Describe los elementos de una institución, le permiten implementar su misión. Esta arquitectura incluye el catálogo de servicios misionales; el modelo estratégico; el catálogo de procesos misionales, estratégicos y de soporte; la estructura organizacional, y el mapa de capacidades institucionales.
Cadena de valor	Relación secuencial y lógica entre insumos, actividades, productos y resultados donde se añade valor a lo largo del proceso de transformación total.
Caracterización de proceso	Representación esquemática de un proceso, permite conocer su objetivo, alcance y sus principales actividades del ciclo PHVA.
Causa	Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
Ciclo PHVA	El ciclo de Deming, también conocido como círculo PDCA corresponde al acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), Ciclo de mejoramiento continuo.
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Consecuencia	Resultado de un evento que afecta los objetivos.
Control	Medida que modifica el riesgo.
Criterios del riesgo	Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
Dato	Un dato por sí mismo no constituye información ni conocimiento, como mínimo requiere una interpretación para poder generar conocimiento y/o información; pero también podría requerir el procesamiento de otros datos y/o metadatos para ser generador de información

Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Dominio	Cada uno de los seis componentes de la estructura de la primera capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
Eficacia	Grado en el cual se realizan las actividades planificadas y se alcanzan los resultados planificados.
Eficiencia	Relación entre el resultado alcanzado y los recursos ejecutados
Estimación del riesgo	Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
Evaluación de riesgos	Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
Evento	Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
Evitación del riesgo	Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
Extracción de Datos	Es el proceso de colección de datos de un sistema de acuerdo con los requerimientos detallados en una especificación funcional. Este proceso puede requerir desarrollo, pruebas y ejecución de programas en uno o varios sistemas.
Factores de Riesgo	Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
Flujos de información	Corresponde a la descripción explicita de la interacción entre proveedores y consumidores de información a lo largo de un proceso o patrón repetible de invocación definido por parte de la Institución.
Generar Valor	Proveer un conjunto de servicios y productos para facilitarle a un cliente el logro de un objetivo. La generación de valor es donde los clientes perciban los beneficios de una iniciativa de arquitectura.
Gestión de la Tecnología	Permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas. (MinTIC, 2015)
Gestión de riesgos	Es un enfoque estructurado para manejar la incertidumbre relativa a las amenazas o factores de riesgo susceptibles afectar el cumplimiento de los objetivos, buscando disminuir la probabilidad y el impacto de su materialización. Incluye las actividades de identificación, evaluación, tratamiento y, seguimiento y mejora de la eficiencia de los controles.
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
Gobernabilidad	Define la capacidad de una organización para controlar y regular su propio funcionamiento con el fin de evitar los conflictos de intereses relacionados con la división entre los beneficiarios y los actores.
Gobierno de TI	"El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para dirigir y controlar la organización hacía el logro de sus objetivos" (www.iteraprocess.com, s.f.).

Gobierno Digital	Es la estrategia de Ministerio de las TIC, busca construir un Estado más eficiente, más transparente y participativo gracias a las TIC.
Identificación del riesgo	Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
Impacto	Cambio adverso en el nivel de los objetivos del negocio logrados.
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
Información	Unidad básica de conocimiento. Es un conjunto de datos organizados y procesados los cuales Tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades.
Infraestructura	Conjunto de elementos lógicos y físicos permiten una determinada solución funcione adecuadamente, tal y como fue diseñada.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
Interoperabilidad	La interoperabilidad es la acción, operación y colaboración de varias entidades para intercambiar información, permite brindar servicios en línea a los ciudadanos, empresas y otras entidades mediante una sola venta de atención o un solo punto de contacto. Es decir, es la forma de ahorrarle a la gente los desplazamientos de un lugar a otro a la hora de realizar un trámite y de hacer el proceso menos engorroso.
Mapa de Ruta	El principal entregable de la arquitectura empresarial es el mapa de ruta. Después de evaluar el estado actual (AS-IS) y establecer la situación objetivo donde se quiere llegar (TO-BE),
Marco de Referencia de Arquitectura Empresarial	Es el instrumento principal, la carta de navegación, para implementar la Arquitectura TI de Colombia. Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información
Matriz de riesgos	Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
Monitoreo	Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
Nivel de riesgo	Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
Plataforma	Es un sistema, sirve como base para hacer funcionar determinados módulos de hardware o de software compatibles.
Proceso	Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
Producto	Son los bienes y servicios, se obtienen de la transformación de los insumos a través de la ejecución de las actividades.
Propietario del riesgo	Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

quick wins o "victorias rápidas"	Son una herramienta profesional para conseguir resultados de una forma rápida y con una inversión generalmente baja dentro de una empresa
Reducción del riesgo	Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
Resultados	Son los cambios en las condiciones del sujeto de beneficio enmarcadas en el objetivo general del proyecto, por efecto del consumo de los productos y el cumplimiento de los supuestos considerados en el mismo.
Retención del riesgo	Aceptación de la pérdida o ganancia proveniente de un riesgo particular
Riesgo	Efecto de la incertidumbre sobre los objetivos. (ICONTEC, 2011)
Riesgo en la seguridad de la información	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
Riesgo Inherente	Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
Riesgo Residual	El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
RPO Recovery Point Objective	Se refiere al volumen de datos en riesgo de pérdida, los cuales la organización considera tolerable. ¿Las transacciones de cuánto Tiempo se está dispuesto a perder, o a reintroducir al sistema?
RTO Recovery TIme Objective	Expresa el Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.
Seguimiento	Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Servicios de TI	Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios TI, se produce valor a la organización. Los servicios de información son casos particulares de servicios de TI.
Servicios Digitales	Permiten a los grupos de interés interactuar con otros sistemas de información de la entidad, del sector, del Estado y con el ciudadano; consumiendo y proporcionando información, a través de servicios disponibles en la web, en un modelo estructurado de portales de información
Sistemas de Información	Es un conjunto de elementos orientados al tratamiento y administración de datos, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Sistemas de Información Misionales	Soportan la misión de la entidad, procesando de manera eficaz las transacciones del negocio, actualizando bases de datos, controlando procesos operativos, generando documentación del negocio y recopilando información sectorial, entre otras responsabilidades, las cuales dependen del Tipo de misión de la Institución.
Transferencia del riesgo	Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Transparencia	De acuerdo con la Corporación Transparencia por Colombia (2010), la transparencia es el "marco jurídico, político, ético y organizativo de la administración pública", las cuales regir las actuaciones de todos los servidores públicos en Colombia, implica gobernar expuesto y a modo de vitrina, al escrutinio público.
Tratamiento del Riesgo	Proceso para modificar el riesgo" (Icontec Internacional, 2011).
Valoración del Riesgo	Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
Vulnerabilidad	Es aquella debilidad de un activo o grupo de activos de información

Derechos de Autor

Introducción

En la actualidad el gran avance de la tecnología ha tenido un impacto significativo en todos los frentes permitiendo agilizar y perfeccionar tareas, mejorando la calidad de procesos, productos y servicios; por tal motivo ha sido muy bien recibida, ubicando a la humanidad en un escenario de globalización digital facilitando el acceso e intercambio de información.

La gestión de riesgos de seguridad de la información inicia con la identificación de los activos de información de la entidad y termina con el plan de tratamiento de los riesgos a los cuales están expuestos dichos activos, siguiendo las normas vigentes, la metodología definida por la entidad para la gestión del riesgo, las pautas y recomendaciones previstas en la ISO 27005 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información. El análisis de riesgos de los activos de información permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Hoy día, todas las instituciones están inmersas en la denominada revolución digital y esto hace el reconocimiento de la importancia de la información en sus procesos misionales y la importancia de tener su información interna bien identificada y protegida, al igual, la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, los cuales obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

Estas mismas ventajas, han traído consigo nuevos retos para protegerla por ser un activo primordial el cual puede ser aprovechado con fines adversos; esto conlleva a plantear un Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el cual se determine implementar herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros para proteger la información y la infraestructura tecnológica soporte y así mitigar los riesgos con procesos de desarrollo de opciones y acciones para mejorarán las oportunidades y reducirán el impacto negativo o la probabilidad de ocurrencia de un evento, dado pie al fortalecimiento de modelos y técnicas enfocados en

la seguridad de la información y su aplicación en espacios donde anteriormente no era indispensable, requiriendo de los profesionales en esta área, la identificación de escenarios donde la seguridad de la información esté ausente o no se aplique de manera adecuada con el fin de concientizar a los actores relacionados de la necesidad de su implementación como también de adaptar modelos y técnicas a estos nuevos ambientes para así mitigar los riesgos.

La Seguridad de la Información en las instituciones tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, permitiendo gestionar y reducir los riesgos e impactos y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

El plan de tratamiento de riesgos de seguridad y privacidad de la información, se basa en una orientación estratégica, cuyo requerimiento principal es el desarrollo de una cultura de carácter preventivo, de tal manera, al comprender el concepto de riesgo, así como el contexto, se planean acciones para reducir la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones de vulnerabilidad para el cumplimiento de los objetivos institucionales.

Con lo anterior, la Institución en pos de dar cumplimiento a la normatividad nacional en estos temas como lo son el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de la Información de la Institución, el decreto 1008 de 14 de junio 2018, de adoptar las buenas prácticas y los lineamientos de los estándares NTC ISO IEC 27001:2013, NTC ISO 31000:2018 entre otros y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP. determina la necesidad de definir el Plan de Tratamiento de Riesgos de Información, convirtiéndose en una carta de navegación para la identificación, análisis, valoración y tratamiento de riesgos relacionados con la información institucional ya sea física o digital, en cada uno de sus procesos, con el fin de garantizar la seguridad en términos de:

- **Confidencialidad:** propiedad de la información para ser concedida únicamente a quien esté autorizado.
- **Integridad:** propiedad de la información de mantenerse exacta y completa.

- **Disponibilidad:** propiedad de la información para ser accesible y utilizable en el momento de ser requerida.

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:

Tabla 1. Criterios de Clasificación

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

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

Tabla 2. Niveles 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.

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

1 Objetivo.

A través de ésta documento se busca orientar a los miembros de Institución 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 la Institución lograr vincular la identificación y análisis de Riesgos hacia los temas de la Seguridad de la Información.

1.1 Objetivos Generales.

Brindar al Instituto Técnico Agrícola (ITA) una herramienta con las pautas necesarias para el adecuado tratamiento de los riesgos expuestos de los activos de información, permitiendo una adecuada toma de decisiones para disminuir la probabilidad materializada en una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la Institución, así como permitir la recuperación del sistema o la trasferencia del problema a un tercero,

con un enfoque sistemático para aplicar los lineamientos de manera integral sobre los riesgos expuestos de Seguridad y Privacidad de la Información y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

1.2 Objetivos específicos de la guía metodológica de riesgos

- Brindar lineamientos y principios para la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Identificar, valorar y clasificar los riesgos de seguridad digital de la Institución para fortalecer el sistema de gestión de riesgos, incorporando controles y medidas de seguridad de la información acordes al entorno operativo de la Institución.
- Identificar, valorar y clasificar los riesgos de seguridad digital de la Institución y así proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Evaluar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento de riesgos de seguridad de la información y con ello reducir toda posibilidad de una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información para lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad/posibilidad e impacto residual de los riesgos al nivel aceptable por parte de la Dirección de la Institución.
- Definir un cronograma de actividades, permitiendo la administración y gestión de los riesgos de la Institución a nivel de Seguridad de la Información.

2 Alcance

El plan de tratamiento de riesgos definido en este documento, pretende realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, permitiendo integrar en los procesos de la entidad, buenas prácticas para contribuir a la toma de decisiones y prevenir incidentes para el logro de los objetivos. Este plan, aplica para los riesgos de seguridad físico o digital y su estructura soporte, identificados

para el proceso de apoyo Gestión de Seguridad de la Información y Recursos Tecnológicos de la Instituto.

La gestión de riesgos de seguridad de la información y su tratamiento, será aplicada sobre cualquier proceso de la Institución y cualquier activo de información de la Institución afectado en su disponibilidad, integridad, confidencialidad, a través de los principios básicos y metodológicos para la gestión de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios para permitir y facilitar el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

Para el Plan de Tratamiento de Riesgos se tendrán en cuenta los riesgos de niveles alto y extremo, los criterios para la evaluación y aceptación de riesgos acorde con los lineamientos definidos por la Institución, los riesgos de niveles inferiores serán aceptados por la Institución.

3 Marco normativo y referencia

Los siguientes documentos de referencia, normativos, vinculantes hacen parte integral del presente documento, sus consideraciones, alcance y construcción:

Marco normativo	Descripción
Constitución Política de Colombia 1991	Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
Decreto 612 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.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 23 de 1982	Propiedad Intelectual - Derechos de Autor.
Ley 594 de 2000	Ley General de Archivos.
Ley 527 de 1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley Estatutaria 1266 de 2008	Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1273 de 2009	Delitos Informáticos protección de la información y los datos.
Ley 1437 de 2011	Código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1581 de 2012	Protección de Datos personales.
Decreto 2609 de 2012	Por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
Decreto 1377 de 2013	Por la cual se reglamenta la ley 1581 de 2012
Ley 1712 de 2014	De transparencia y del derecho de acceso a la información pública nacional
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea
Ley 1341 de 2009	Tecnologías de la Información y aplicación de seguridad.
Decreto 2952 de 2010	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012
Decreto 1083 de 2015	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa
CONPES 3854 de 2016	Política Nacional de Seguridad digital,
Resolución 79B de 2020	Por la cual se crea el Comité de Seguridad de la Información de la Institución
Resolución 289 de 2019	Por la cual se adopta la Política General del Modelo de Seguridad y Privacidad de la Información y el Manual de la Política Seguridad y Privacidad de la Información de la Institución
Resolución 290 de 2019	Por la cual se adopta la Política de tratamiento y Protección de datos personales de la Institución
Resolución P4042 de 2019	Por medio de la cual se crea, organiza y conforma un grupo interno de trabajo de seguridad de la Información y Protección de Datos personales y se asignan funciones de coordinador a un empleado público de la Institución

4 Requisitos técnicos

- **NTC ISO IEC 27001** Sistemas de gestión de la seguridad de la información
- **GTC ISO IEC 27002** Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información
- **NTC ISO IEC 27005** Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- **NTC ISO 19011** Directrices para la Auditoria de los Sistemas de Gestión.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas

5 Modelo Integrado de Planeación y Gestión (MIPG).

5.1 Contexto normativo.

El Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.

Ilustración 1. Articulación de los sistemas de Gestión y de Control Interno
Fuente: Función Pública, 2017

En el Sistema de Gestión están contemplados todas las entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad. El Sistema de Gestión se complementa y articula con otros sistemas, modelos y estrategias que establecen lineamientos y directrices en materia de gestión y desempeño para las entidades públicas, tales como el Sistema Nacional de Servicio al Ciudadano y el Sistema de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. Así mismo, es compatible con los modelos de acreditación específicos, establecidos para los sectores de Educación y Salud.

5.2 ¿Qué es Modelo Integrado de Planeación y Gestión (MIPG)?

Este modelo es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, tiene el fin de generar resultados en atención a los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio (Manual operativo MIPG, marzo 2021 v4).

El MIPG es en sí mismo un modelo de gestión de calidad ya que se fundamenta en generar resultados que satisfagan las necesidades y atiendan los problemas de los ciudadanos. Es en torno a estos resultados que deben girar todas sus actuaciones y decisiones.

Ilustración 2. Definición del Modelo Integrado de Planeación y Gestión –MIPG
Fuente: Departamento Administrativo de la Función Pública, MIPG, 2021.

Además el MIPG es:

- Un marco de referencia porque contempla un conjunto de conceptos, elementos, criterios, que permiten llevar a cabo la gestión de las entidades públicas.
- Enmarca la gestión en la calidad y la integridad, al buscar su mejoramiento permanentemente para garantizar los derechos, satisfacer las necesidades y expectativas de la ciudadanía.
- El fin de la gestión es generar resultados con valores, es decir, bienes y servicios que tengan efecto en el mejoramiento del bienestar de los ciudadanos, obtenidos en el marco de los valores del servicio público (Honestidad, Respeto, Compromiso, Diligencia y Justicia).
- Busca generar valor público a través de la entrega de resultados que respondan y satisfagan las necesidades y demandas de los ciudadanos.

El MIPG funciona mediante tres componentes, una institucionalidad, una operación y una medición.

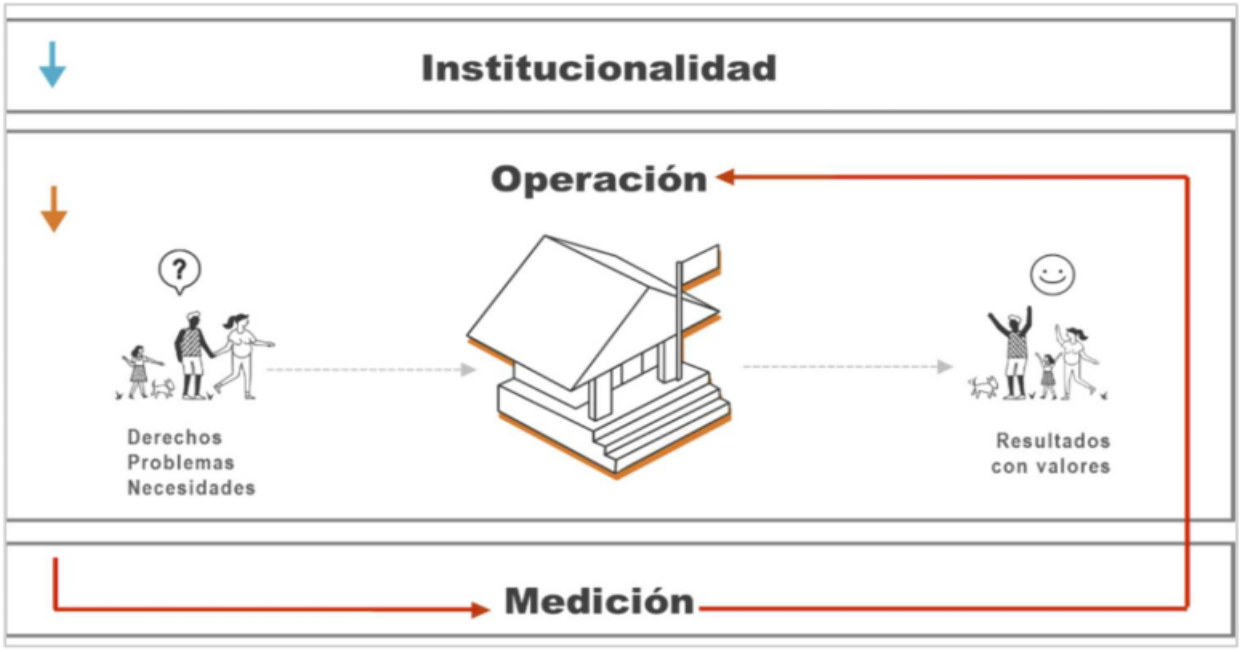

Ilustración 3. Funcionamiento de MIPG
Fuente: Departamento Administrativo de la Función Pública, MIPG, 2021.

Institucionalidad. Conjunto de instancias que trabajan coordinadamente para establecer las reglas, condiciones, políticas, metodologías para que el Modelo funcione y logre sus objetivos, dichas instancias son:

- Comités Sectoriales de Gestión y Desempeño.
- Comités Territoriales de Gestión y Desempeño.
- Comité Institucional de Gestión y Desempeño

Operación. MIPG opera a través de un conjunto de 7 dimensiones que agrupan las políticas de gestión y desempeño institucional (Talento Humano, Direccionamiento estratégico y Planeación, Gestión con valores para resultados, Evaluación de resultados, Información y comunicación, Gestión del conocimiento y Control Interno), implementadas de manera articulada e intercomunicada, permitirán que MIPG funcione.

El modelo se concentra en las prácticas y procesos que adelantan las entidades públicas para transformar insumos en resultados que produzcan los impactos deseados, esto es, una gestión y un desempeño institucional que generan valor público.

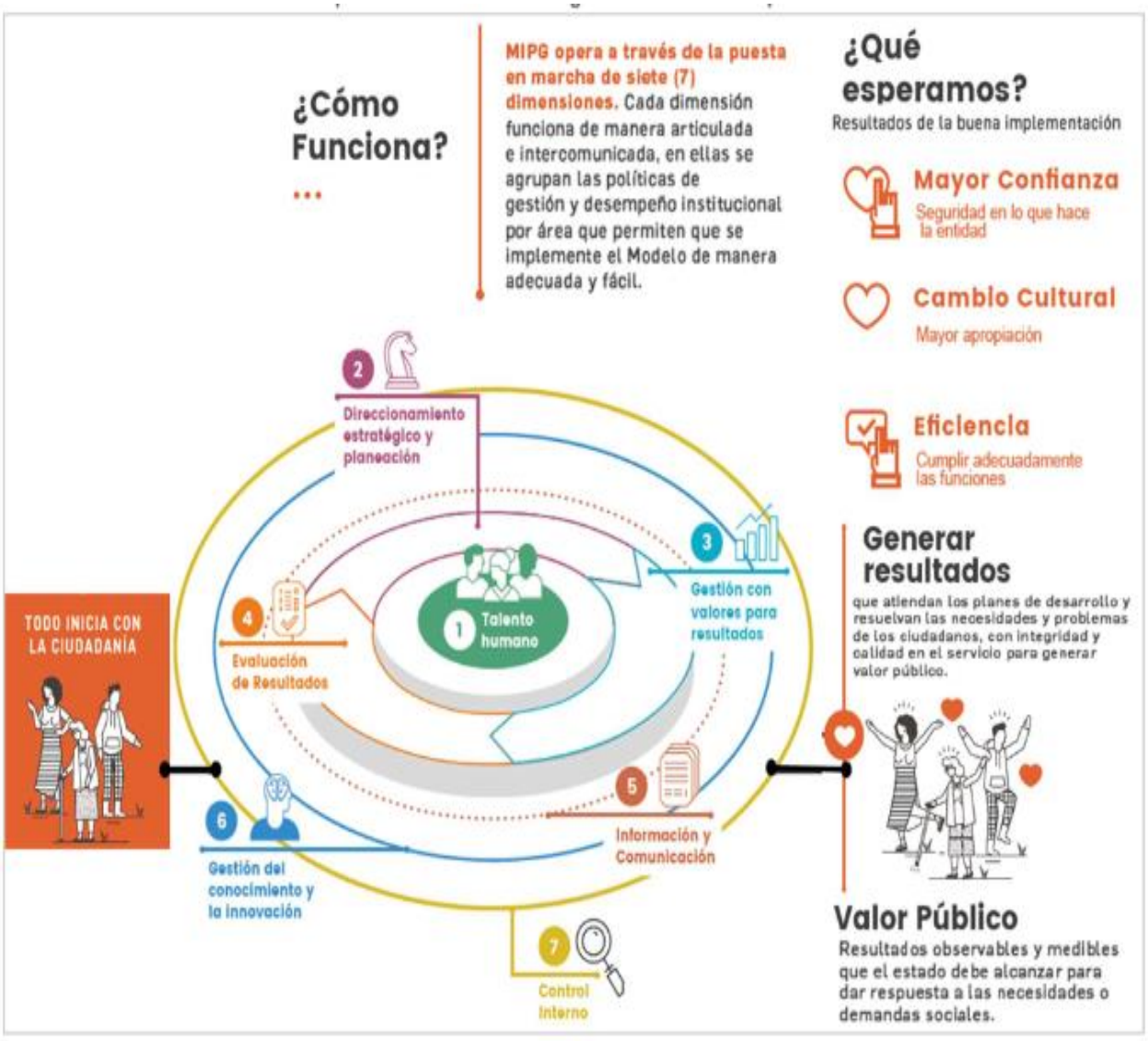

Ilustración 4. Operación del Modelo Integrado de Planeación y Gestión –MIPG
Fuente: Departamento Administrativo de la Función Pública, MIPG, 2021.

Medición del desempeño institucional MDI. Es un ejercicio anual que busca determinar el estado de la gestión y desempeño de las entidades públicas del orden nacional y territorial, bajo los criterios y estructura de Modelo Integrado de Planeación y Gestión – MIPG (evaluación de las políticas).

Busca también medir el avance del Sistema de Control Interno implementado a través del Modelo Estándar de Control Interno - MECI.

6 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 para permitir a la Institución 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" como se menciona en la guía, tener el verdadero compromiso de los directivos garantizan en gran medida el éxito de cualquier proceso emprendido, se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona en el Modelo de Seguridad y Privacidad de la Información (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 a cargo el desarrollo o sostenimiento del Modelo Estándar de Control Interno (MECI) y el Sistema de Gestión de la Calidad) para asesorar y apoyar todo el proceso de diseño e implementación del Componente, el MSPI se acoge pues se busca 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, por esta razón, se deben incluir los riesgos de seguridad en el momento de hacer 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 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.

7 Políticas de Administración de Riesgos

Las políticas de administración de riesgos 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 por que 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.

7.1 Consolidación delas Políticas.

Para la consolidación de las Políticas de Administración de Riesgos se deben tener en cuenta todas las etapas anteriormente desarrolladas.

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

El Comité de Seguridad de la Información de la Institución, a través del sistema de gestión de seguridad de la información, se compromete a mantener la cultura de la gestión de riesgos asociados, con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos de TI, gestionando los riesgos de los procesos y proyectos, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de amenazas asociadas a los activos de información que comprometan la disponibilidad, confidencialidad e integridad, fortaleciendo las medidas de control de manera continua y oportuna

La política define los lineamientos para la gestión de los riesgos y establece pautas de acción necesarias para todos los funcionarios administrativos, docentes, contratistas y/o terceros que requieran acceso a los sistemas de información o aplicaciones de la Institución.

Las opciones para el tratamiento del riesgo se deben seleccionar con base en el resultado de la valoración del riesgo, el costo esperado de implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Así mismo, el Comité de Seguridad de la Información de la Institución actualizar la política de administración de los riesgos de la Institución para la gestión del cumplimiento a las diferentes normas, legales, técnicas o sistemas de gestión implementados, y los cuales se orientan según la guía para la administración del riesgo de la Función Pública, a excepción de los riesgos de seguridad y salud en el trabajo, los cuales disponen su propia metodología.

Las siguientes son las alternativas planteadas para el tratamiento del riesgo:

Alternativas planteadas para el tratamiento del riesgo

Reducir o Mitigar el riesgo.	Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo, mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.
Retener o Aceptar el riesgo.	Aceptación de la pérdida o ganancia proveniente de un riesgo particular. La decisión sobre la retención sin acción posterior se debe tomar dependiendo la evaluación del riesgo.
Evitar el riesgo.	Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación, se debe evitar la actividad o acción que da origen al riesgo en particular.
Transferir o Compartir el riesgo.	Compartir con otra de las partes la pérdida o la ganancia de un riesgo. El riesgo se debe transferir a otra persona que pueda gestionar de manera más eficaz el riesgo en particular dependiendo la evaluación del riesgo.

7.2 Formulación de las políticas

Está a cargo del Representante Legal de la entidad y el Comité de Coordinación de Control Interno y se basa en el mapa de riesgos construido durante el proceso; la política señala qué debe hacerse para efectuar el control y su seguimiento, basándose en los planes estratégicos y los objetivos institucionales o por procesos.

Debe contener los siguientes aspectos:

- Los objetivos que se esperan lograr.
- Las estrategias para establecer cómo se van a desarrollar las política, a largo, mediano y corto plazo.
- Los riesgos que se van a controlar.
- Las acciones a desarrollar contemplando el tiempo, los recursos, los responsables y el talento humano requerido.
- El seguimiento y evaluación a la implementación y efectividad de las políticas

8 Visión general del proceso GRSPI

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación se puede observar la estructura completa con sus desarrollos básicos:

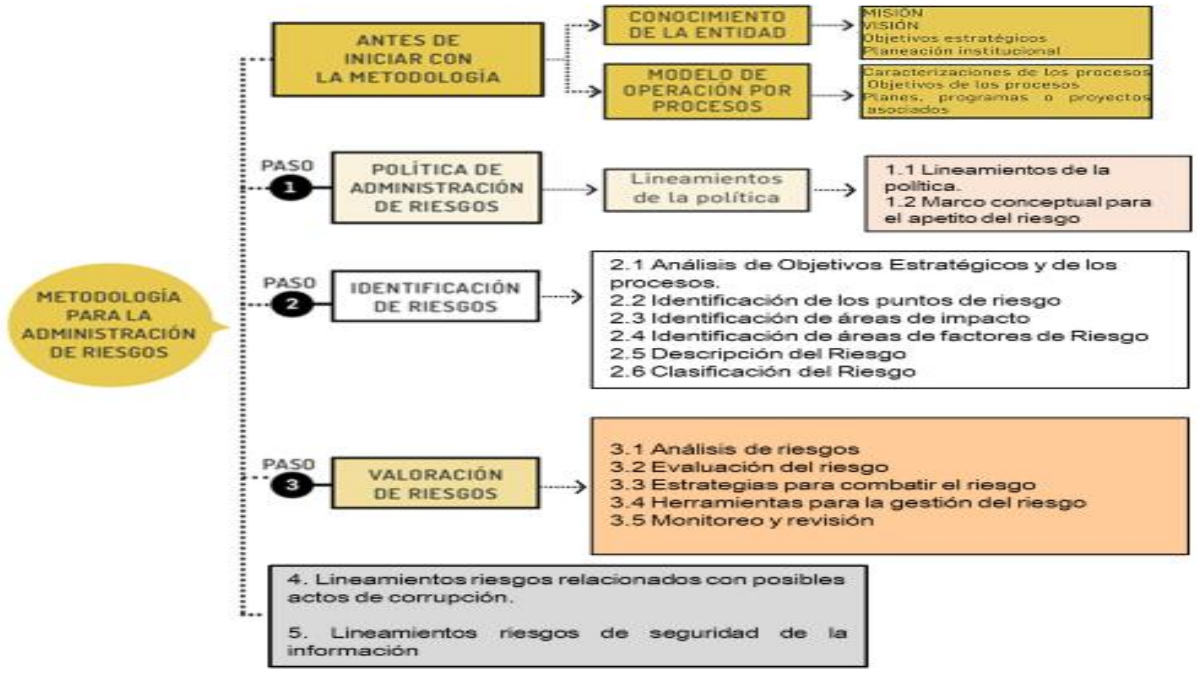

Ilustración 5. Metodología para la administración del riesgo
Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

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.

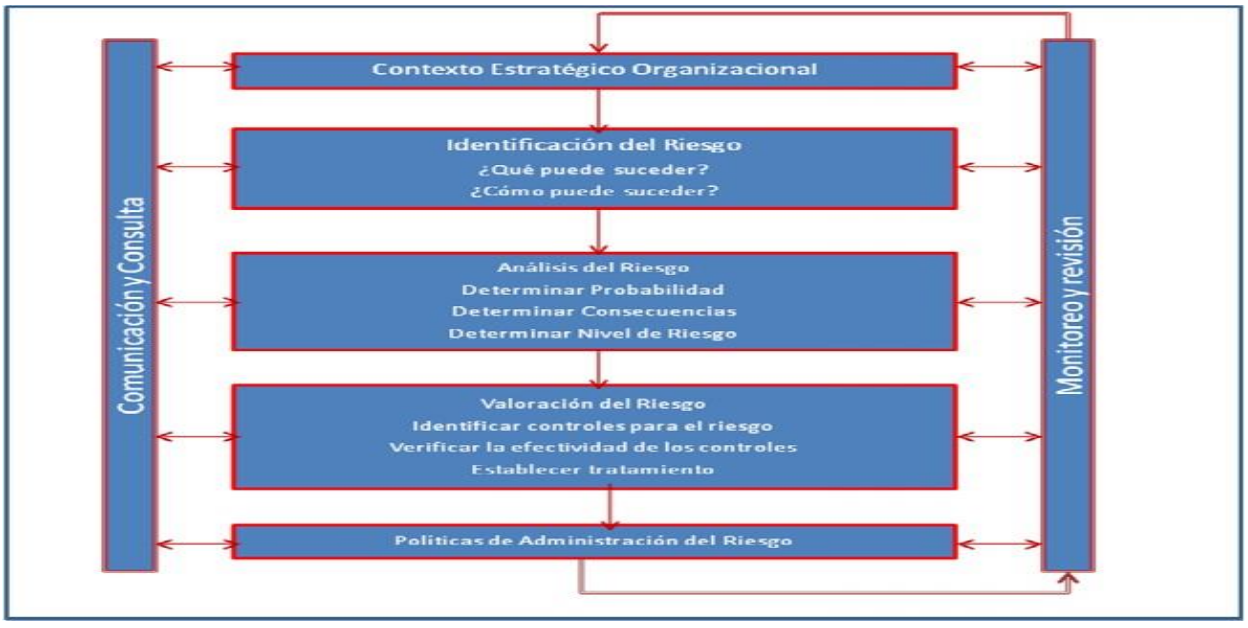

Ilustración 6. Proceso para la administración del riesgo

Fuente: Cartilla de Administración de Riesgos del DAFP

La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

A continuación, se presenta 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 la seguridad de la información; los elementos que lo componen son:

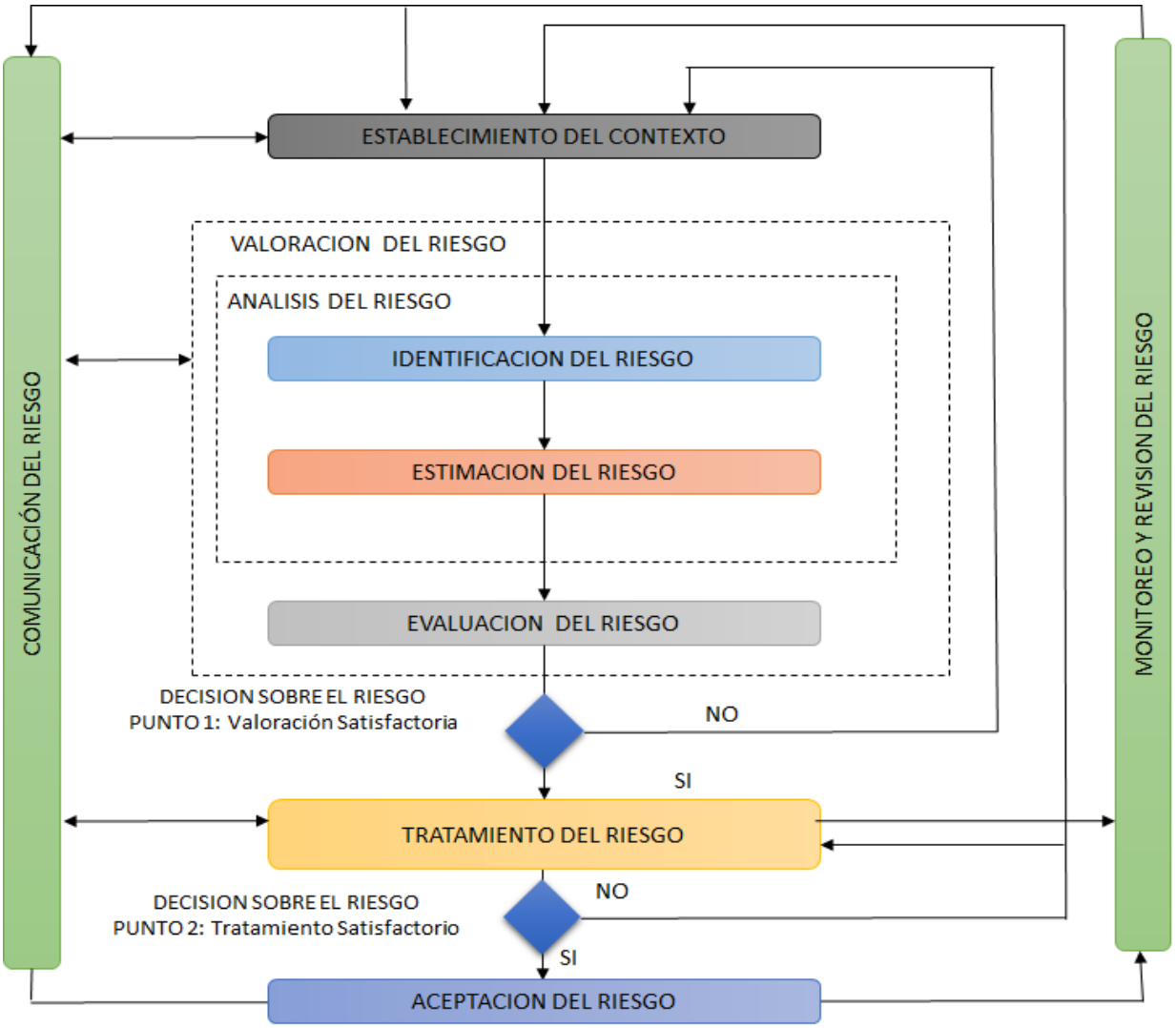

Ilustración 7. Proceso de gestión de riesgo en la seguridad y privacidad de la información
Fuente: Norma NTC ISO IEC 27005

Así como se ilustra, 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.

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

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

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

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.

9 Criterios básicos

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.

9.1 Establecimiento del contexto.

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la Institución y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en sus procesos, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Institución.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

9.1.1 Criterios de evaluación.

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

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

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

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

9.1.2 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 impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

9.1.3 Criterios de Aceptación.

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 dependerán con frecuencia de las políticas, metas, objetivos de la Institución y de las partes interesadas.

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

10 Valoración de los riesgos.

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.

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Institución, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
- Identificación de los riesgos

- Estimación del riesgo
- Evaluación del riesgo.

10.1 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.

10.2 Identificación de riesgos y oportunidades

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.

Para la evaluación de riesgos de seguridad de la información en primer lugar se deben identificar los activos de información por proceso en evaluación.

10.2.1 Identificación de activos de información,

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, se clasifican en dos tipos:

a) **Primarios**:

- **Actividades y procesos del negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión institucional; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la Institución; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- **Información**: información vital para la ejecución de la misión institucional; información personal que se puede definir

específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

b) **De Soporte**

- **Hardware**: consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- **Software**: consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- **Redes**: consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- **Personal**: consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- **Ubicación**: comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- **Estructura organizativa**: responsables, dependencias, contratistas, etc.

Una vez identificados los activos de información se deben priorizar de acuerdo a su impacto sobre el sistema de gestión de seguridad de la información (valor económico, confidencialidad, integridad y disponibilidad).

10.2.2 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.

Identificados los activos de información y de tener el resultado de la priorización del impacto sobre el sistema de gestión de la seguridad de la información, se deben identificar las amenazas que pueden causar daños en los activos de

información primarios y/o de soporte de mayor impacto. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc. A continuación se describen una serie de amenazas comunes.

Tabla 4. Amenazas Comunes

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	

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

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

FUENTE DE AMENAZA	MOTIVACIÓN	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 extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados,	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto

negligentes, deshonestos o despedidos)	ingreso de datos, error de programación)	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.

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

10.2.3 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.

10.2.4 Valoración de controles para el tratamiento de riesgos.

Esta etapa se debe tener en cuenta la evaluación realizada, 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.

La siguiente tabla, muestra la organización de los controles detallando los dominios definidos en el componente de Planificación. SIEMPRE se deben mencionar los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001, cual trata de los objetivos de control,

Tabla 5. Estructura de controles.

Núm.	Nombre	Control	Dominio	Seleccionado/ Excepción	Descripción / Justificación

Fuente: Construcción propia (error encontrado en la Guía 8 - Controles de Seguridad y Privacidad de la Información. MinTIC 2016

Cada campo se define así:

- **Núm.:** Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- **Nombre:** Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- **Control:** Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.
- **Dominio:** Este campo describe si el control aplica para uno o múltiples dominios.
- **Seleccionado / Excepción:** El listado de controles además debe ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.
- **Descripción / Justificación**: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado.

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:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

- **Correctivos:** aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.

El procedimiento para la valoración del riesgo parte de la evaluación de los controles existentes, lo cual implica:

a) Describirlos (estableciendo si son preventivos o correctivos).
b) Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.
c) Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la Matriz de Calificación, Evaluación y Respuesta a los Riesgos es posible desplazarse (Los controles luego de su valoración permiten desplazarse en la matriz, de acuerdo a si cubren probabilidad o impacto, en el caso de la probabilidad desplazaría casillas hacia arriba y en el caso del impacto, hacia la izquierda como se muestra en el gráfico, de acuerdo a la valoración de controles), a fin de bajar el nivel de riesgo al que está expuesto el proceso analizado.

Tabla 6. Valoración - Evaluación

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

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

Por otro lado, la guía facilita las siguientes herramientas con las cuales se logra hacer una cuantificación del análisis de los controles elegidos, para lo cual n se muestran dos cuadros orientadores para ponderar de manera objetiva los controles y poder determinar el desplazamiento dentro de la Matriz de Calificación, Evaluación y Respuesta a los Riesgo

Tabla 7. Valoración de controles

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
	Posee una herramienta para ejercer el control.			15

Herramientas para ejercer el control	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 la ejecución del con- trol y seguimiento es adecuada.			25
	TOTAL			**100**

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

Tabla 8. Rangos de calificación de los controles

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 para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

El resultado obtenido a través de la valoración del riesgo es denominado también tratamiento del riesgo, ya que se "involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones"22, así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará finalmente la selección de la opciones de tratamiento del riesgo, así:

- Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc. Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

- Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
- Asumir un riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Dicha selección implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar los siguientes aspectos como:

- Viabilidad jurídica.
- Viabilidad técnica.
- Viabilidad institucional.
- Viabilidad financiera o económica.
- Análisis de costo-beneficio.

Una vez implantadas las acciones para el manejo de los riesgos, la valoración después de controles se denomina riesgo residual, este se define como aquel que permanece después que la dirección desarrolle sus respuestas a los riesgos.

10.2.5 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 sí 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.

Tabla 9. Identificación de las vulnerabilidades y amenazas.

TIPO DE ACTIVO	EJEMPLOS	
	VULNERABILIDADES	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

Fuente: Construcción propia, Información tomada de la Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

10.2.6 Métodos para la valoración de las vulnerabilidades técnicas:

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación del modelo de seguridad en las entidades.

Esta metodología ha sido diseñada para ayudar a las entidades a entender y comprender, la realización de unas pruebas, los objetivos de las mismas y el beneficio que se obtiene al identificar sus etapas y gestionarlas.

Esta metodología es desarrollada en diferentes etapas que permiten concluir que tanto ha avanzado la entidad con la implementación del modelo; de esta manera, a través de la valoración de diferentes aspectos se permitirá identificar vulnerabilidades y amenazas a las cuales está expuesta la entidad, así como también posibles debilidades en los controles implementados.

Al igual que los demás procedimientos planteados en el modelo de seguridad y privacidad de la información, se busca proteger la disponibilidad, integridad y confidencialidad de la información de la entidad.

Un factor externo de mucho impacto, que se alinea con la ejecución de las pruebas de seguridad y privacidad y sus resultados, son los intereses de lo que se denomina Alta Dirección, que para nuestro caso son los directivos de las entidades del estado, estos se ven reflejados en las capacidades de las entidades de llevar a buen término la implementación del modelo de seguridad para dar cumplimiento a la normatividad vigente; así como llevar a la entidad al siguiente nivel de seguridad que permite que sus procesos y atención al

ciudadano deje una buena imagen en la sociedad colombiana. (Ver guía de pruebas de efectividad. MinTIC, 2016)

10.2.7 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.

Posterior a la identificación del listado de activos, sus amenazas y los controles y medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Institución. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

10.3 Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad/posibilidad 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 de estos. 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:

- Posibilidad: la posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse y que tan posible es que la amenaza explote la vulnerabilidad sobre el activo de información.
- Impacto: hace referencia a las consecuencias que puede ocasionar al Instituto Técnico Agrícola (ITA) la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la posibilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

Para realizar el análisis de riesgo de un proceso, se deberá calificar el impacto y la posibilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos los cuales pueden ser valorados de manera cualitativa y/o cuantitativa.

Para la estimación de la posibilidad se van a utilizar la metodología de valoración cualitativa:

Tabla 10. Valoración Posibilidad

Estimación del Riesgo: POSIBILIDAD			
Posibilidad	Valor	Descripción	Frecuencia
Casi Seguro	A	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Probable	B	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Posible	C	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Improbable	D	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Raro	E	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

Para la estimación de la consecuencia/impacto se va a utilizar la metodología de valoración cuantitativa:

Tabla 11. Valoración Impacto

Estimación del Riesgo: CONSECUENCIA - IMPACTO		
Posibilidad	Valor	Descripción
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	2	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Institución. Tiene un impacto bajo en los procesos de otras áreas de la Institución.
Moderado	3	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Institución. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	4	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la Institución** y tiene un **impacto significativo en la imagen pública** de la Institución. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	5	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Institución**, tiene un **impacto catastrófico en la imagen pública de la Institución**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

10.3.1 Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su posibilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la Institución. La exposición al riesgo es la ponderación de la posibilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo,

moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Tabla 12.Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional.

EVALUACION DEL RIESGO - CONSECUENCIA NEGATIVA					
POSIBILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Las zonas de riesgo se diferencian por colores y por número de la zona de la siguiente manera:

Tabla 13. Convención Zonas de Riesgo

B. Zona de riesgo baja:	Asumir el riesgo
M. Zona de riesgo moderado:	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

El análisis del riesgo permite además identificar oportunidades de mejora, cuando la consecuencia es positiva:

Tabla 14. Esquema general de Matriz de Oportunidad Institucional y Zonas de Oportunidad Institucional.

EVALUACION DEL RIESGO - CONSECUENCIA POSITIVA					
POSIBILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Las zonas de oportunidad se diferencian por colores y por número de la zona de la siguiente manera:

Tabla 15. Convención Zonas de Oportunidad

B: Zona de oportunidad baja:	Asumir la oportunidad
M: Zona de oportunidad moderada:	Asumir la oportunidad.
A: Zona de oportunidad Alta:	Aumentar la posibilidad de ocurrencia, compartir o transferir
E: Zona de oportunidad extrema:	Aumentar la posibilidad de ocurrencia y/o el impacto de la oportunidad, asumir, compartir o transferir.

10.4 Evaluación de los riesgos

Una vez se valoran los impactos, la posibilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo y oportunidades, para los cuales se deberán comparar frente a los criterios de evaluación definidos en el contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto Alto o aprovechar la oportunidad.

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:

- "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", 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.

Para determinar el impacto se pueden utilizar las siguientes tablas que representan los temas en que suelen impactar la ocurrencia de los riesgos y se asocian con la clasificación del riesgo previamente realizada, y se relaciona con las consecuencias potenciales del riesgo identificado. Las tablas propuestas representan los impactos de mayor ocurrencia en las entidades del Estado, no obstante cada entidad puede incluir otros tipos de impacto según su particularidad.

NIVEL	IMPACTO

	CONFIDENCIALIDAD EN LA INFORMACIÓN	CREDIBILIDAD O IMAGEN	LEGAL	OPERATIVO
1	Personal	Grupo de funcionarios	Multas	Ajustes a una actividad concreta
2	Grupo de Trabajo	Todos los funcionarios	Demandas	Cambios en los procedimientos
3	Relativa al Proceso	Usuarios ciudad	Investigación Disciplinaria	Cambios en la interacción de los procesos
4	Institucional	Usuarios región	Investigación Fiscal	Intermitencia en el servicio
5	Estratégica	Usuarios país	Intervención – Sanción	Paro total del proceso

Fuente: Construcción Propia, Información tomada de Guía para la administración del riesgo– Departamento Administrativo de la Función Pública (DAFP)

- **El impacto de confidencialidad de la información** se refiere a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.
- **El impacto de credibilidad** se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad
- **El impacto legal** se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable
- **El impacto operativo** aplica en la mayoría de las entidades para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos.

Ahora bien, considerando que para un proceso es posible analizar más de un impacto, se pueden ir agrupando en el siguiente cuadro, en el cual se establecen concretamente

En el ejemplo se muestra el análisis sobre el impacto de Credibilidad o imagen. En este mismo sentido se pueden incluir otros impactos del proceso que se esté analizando.

Tabla 16. Análisis sobre el impacto de Credibilidad o imagen

TIPO DE IMPACTO	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
Imagen	Se afectó al grupo de	Se afectó a todos los	Se afectó a los usuarios locales.	Se afectó a los usuarios	Se afectó a los usuarios en el

	funcionarios del proceso.	funcionarios de la entidad.		locales y regionales.	orden nacional

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

La Evaluación del Riesgo, permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación a los riesgos, a continuación se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la probabilidad son raras, improbables, posibles, probables y casi seguras.

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 tabla:

Tabla 17. Matriz de calificación, evaluación y repuesta a los riesgo

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 para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

Teniendo en cuenta los pasos mencionados anteriormente, y las herramientas entregadas por la guía, se presenta a continuación el análisis de uno de los riesgos de Seguridad de la Información identificados anteriormente.

Tabla 18.Aplicado a la metodología

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			
Cambio en los datos de contacto de los usuarios	3	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	Zona de Riesgo Extrema	Reducir el Riesgo Evitar Compartir o Transferir

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la Dirección para modificar su probabilidad o impacto

Tabla 19. Análisis del riesgo denominado Riesgo Inherente

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

Fuente: Administración de Riesgos Corporativos. Técnicas de Aplicación Pricewaterhouse Coopers, Colombia. 2005. Página 39

10.4.1 Tratamiento de los riesgos de seguridad y privacidad de la información

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

Basado en el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión importante para la decisión.

De acuerdo a los análisis de costo/beneficio se sugiere como guía las siguientes opciones de tratamiento

Tabla 20. Tratamiento de los riesgos de seguridad y privacidad de la información

COSTO – BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la posibilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas. Se recomienda ver la 27001 para la definición de controles.

11 Comunicación y consulta

Una vez finalizada la etapa de valoración y tratamiento de los riesgos y oportunidades se debe socializar con las partes involucradas para que conozcan de manera integral el estado de seguridad y privacidad de información y se tomen decisiones y se definan los planes de tratamiento.

12 Monitoreo y seguimiento de los riesgos de seguridad y privacidad de la información

Periódicamente 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 como la misma institución por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas, (3) cambios o aparición de nuevas vulnerabilidades, (4) aumento de las consecuencias o impactos, (5) 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.

13 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, 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 21. 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 Probabilidad o Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje e 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
			Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema, generando alarmas ante anomalías	Probabilidad	30	25	55

Fuente: Guía de gestión de riesgos, MinTIC- Guía N° 7, 2016

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:

Tabla 22. 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 para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

Tabla 23. 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

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)

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 Anexo A.

14 Plan de tratamiento de riesgos de seguridad y privacidad de la información

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos y aprovechar las oportunidades, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información:

Tabla 24. Plan de tratamiento de los riesgos de seguridad y privacidad de la información

Gestión de Riesgos				
Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Chief Information Officer (CIO, Grupo de Seguridad de la Información)	02/2023	04/2023
Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y Privacidad de la Información	Chief Information Officer (CIO, Grupo de Seguridad de la Información)	02/2023	04/2023
Identificación de Riesgos de la Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información	Chief Information Officer (CIO, Grupo de Seguridad de la Información)	01/2023	12/2023
	Realimentación, revisión y verificación de los riesgos identificados (ajustes)	Chief Information Officer (CIO, Grupo de Seguridad de la Información)	01/2023	12/2023
Aceptación de los Riesgos Identificados	Aceptación, aprobación de Riesgos identificados y planes de tratamiento	Chief Information Officer (CIO, Grupo de Seguridad de la Información) - Comité de Seguridad de la Información	02/2023	12/2023

Socialización a las partes interesadas	Socialización Matriz de Riesgos	Chief Information Officer (CIO, Grupo de Seguridad de la Información)	03/2023	05/2023
Seguimiento Fase de Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Planeación y Calidad	01/2023	12/2023
Evaluación de riesgos residuales	Evaluación de riesgos residuales	Planeación y Calidad –Control interno	01/2023	12/2023
Mejoramiento	Identificación de oportunidades de mejoras acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	Planeación y Calidad - Chief Information Officer (CIO, Grupo de Seguridad de la Información)	01/2023	12/2023
	Actualización de la Guía de Gestión de Riesgos Seguridad de la Información, de acuerdo a los cambios solicitados	Comité de seguridad de la Información	01/2023	12/2023
Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Gestión TI - Gestión de infraestructura y administración del campus	01/2023	12/2023

Anexo A. Mapa de Riesgos

Tabla 25.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: Cambio en los datos de contacto de los usuarios									
CALIFICACIÓN		Evaluación	CONTROL ES	NUEVA CALIFICACIÓN		Evaluación	Medid as de Respuesta	ACCIONES	RESPONSABLE	INDICADOR
Prob.	Imp.	Zona de Riesgo o		Prob.	Imp.	Zona de Riesgo				
3	4	EXTREMA	Procedimientos establecido s 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 usuario s 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
			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

Fuente: Guía para la administración del riesgo – Departamento Administrativo de la Función Pública (DAFP)