



El futuro digital
es de todos

MinTIC

Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

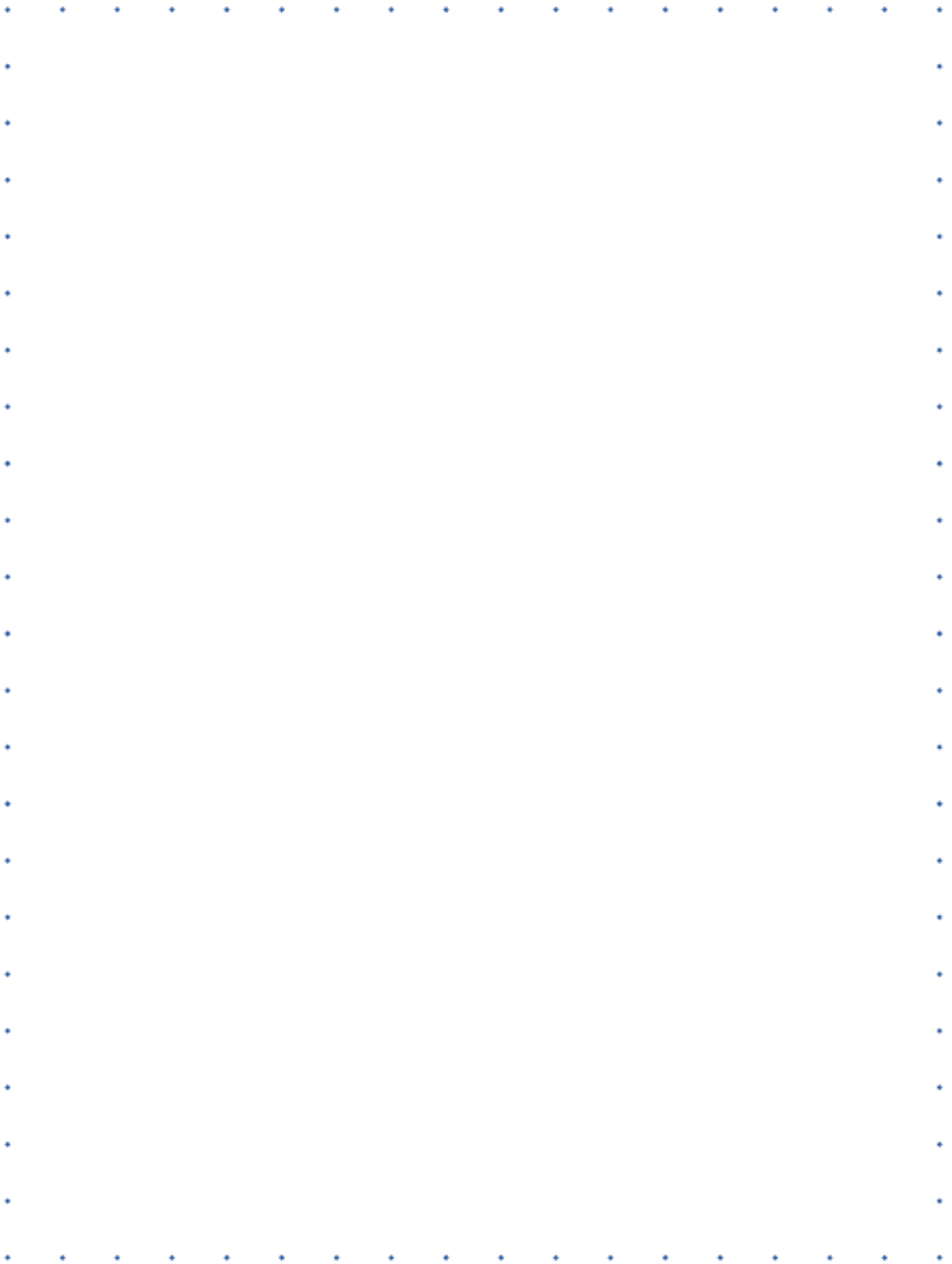
(Anexo 4 – DAFP)

MinTIC – Viceministerio de Transformación
Digital.
Dirección de Gobierno Digital

MINGRSI

Tabla de contenido

1	Generalidades	4
1.1	Derechos de autor	4
1.2	Objetivos.....	4
1.2.1	Objetivo general	4
1.2.2	Objetivos específicos	5
1.3	Alcance del documento	5
1.4	Definiciones.....	5
2	Integración del modelo de seguridad y privacidad de la Información (MSPI).....	6
3	GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA ENTIDADES PÚBLICAS ..	8
3.1	Fase 1. Planificación de la GRSD	8
3.1.1	Contexto interno y externo de la entidad pública	9
	• Establecimiento del contexto externo	9
	• Establecimiento del contexto interno	9
3.1.2	Alcance para aplicar la gestión de riesgos de seguridad de la información.....	10
3.1.3	Alineación o creación de la política de gestión de riesgo de seguridad de la información.	10
3.1.4	Definición de roles y responsabilidades	10
3.1.5	Definición de recursos para la Gestión de riesgos de seguridad de la información	11
3.1.6	Identificación de activos de información.....	11
3.1.7	Identificar los riesgos inherentes de seguridad de la información.....	17
3.1.8	Identificación del nivel de confianza para la autenticación digital.....	27
3.1.9	Identificación y evaluación de los controles existentes	27
3.1.10	Tratamiento de los riesgos de seguridad de la información.....	28
3.1.11	Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo	28
3.2	Fase 2. Ejecución.....	28
3.3	Fase 3. Monitoreo y revisión	29
3.3.1	Registro y reporte de incidentes de seguridad de la información	29
3.3.2	Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública.	29
3.3.3	Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales	30
3.3.4	Auditorías internas y externas	31
3.3.5	Medición del desempeño	31
3.4	Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad de la información	31
4	CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	32



1 Generalidades

1.1 Derechos de autor

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información -MSPI, son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC.

De igual forma, son derechos reservados por parte del MINTIC, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del MSPI publicadas en el compendio de las normas técnicas colombianas vigentes.

En consecuencia, el MINTIC goza de los derechos de autor¹ establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del MNGRSI y su contenido.

Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).

Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la *International Standard Organization* (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el MGRSD y sus documentos o anexos que son de su autoría o propiedad.

1.2 Objetivos

1.2.1 Objetivo general

El objetivo principal de este documento es orientar a todas las entidades públicas del orden nacional y territorial, en la implementación de la Gestión de Riesgos de Seguridad de la información, que permita incrementar la

¹**Ley 1520 de 2012.** Artículo 5. El artículo 12 de la Ley 23 de 1982 quedará así: "Artículo 12. El autor o, en su caso, sus derechohabientes, tienen sobre las obras literarias y artísticas el derecho exclusivo de autorizar, o prohibir: a) La reproducción de la obra bajo cualquier manera o forma, permanente o temporal, mediante cualquier procedimiento incluyendo el almacenamiento temporal en forma electrónica.

Ley 1450 de 2011. Artículo 28. Propiedad intelectual obras en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo. El artículo 20 de la ley 23 de 1982 quedará así: "Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo, el autor es el titular originario de los derechos patrimoniales y morales; pero se presume, salvo pacto en contrario, que los derechos patrimoniales sobre la obra han sido transferidos al en cargante o al empleador, según sea el caso, en la medida necesaria para el ejercicio de sus actividades habituales en la época de creación de la obra. Para que opere esta presunción se requiere que el contrato conste por escrito. El titular de las obras de acuerdo con este artículo podrá intentar directamente o por intermedia persona acciones preservativas contra actos violatorios de los derechos morales informando previamente al autor o autores para evitar duplicidad de acciones".

Ley 23 de 1982. Artículo 30. El autor tendrá sobre su obra un derecho perpetuo, inalienable, e irrenunciable para: a) Reivindicar en todo tiempo la paternidad de su obra y, en especial, para que se indique su nombre o seudónimo cuando se realice cualquiera de los actos mencionados en el artículo 12 de esta ley.

confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades.

1.2.2 Objetivos específicos

- a. Otorgar una herramienta de orientación para la ejecución de la Gestión de Riesgos de Seguridad de la información, en las entidades de Gobierno nacional, territoriales y del sector público en general.
- b. Estandarizar el proceso de Gestión de Riesgos de Seguridad de la información, en las entidades del Gobierno nacional, territoriales y del sector público en general.
- c. Generar mecanismos para que las entidades del Gobierno nacional, territoriales y del sector público en general puedan establecer los elementos para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital.
- d. Proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital.

1.3 Alcance del documento

Este documento complementa y profundiza lo expuesto en la ***Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas***, emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, específicamente en las secciones de Análisis del contexto (con un enfoque hacia el entorno digital), identificación de activos, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad de la información, controles para la mitigación de los riesgos de seguridad de la información, el reporte de riesgos de seguridad de la información y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad de la información adecuada.

1.4 Definiciones

Ver Documento **Modelo de Seguridad y Privacidad de la Información (MSPI)**.

2 Integración del modelo de seguridad y privacidad de la Información (MSPI)

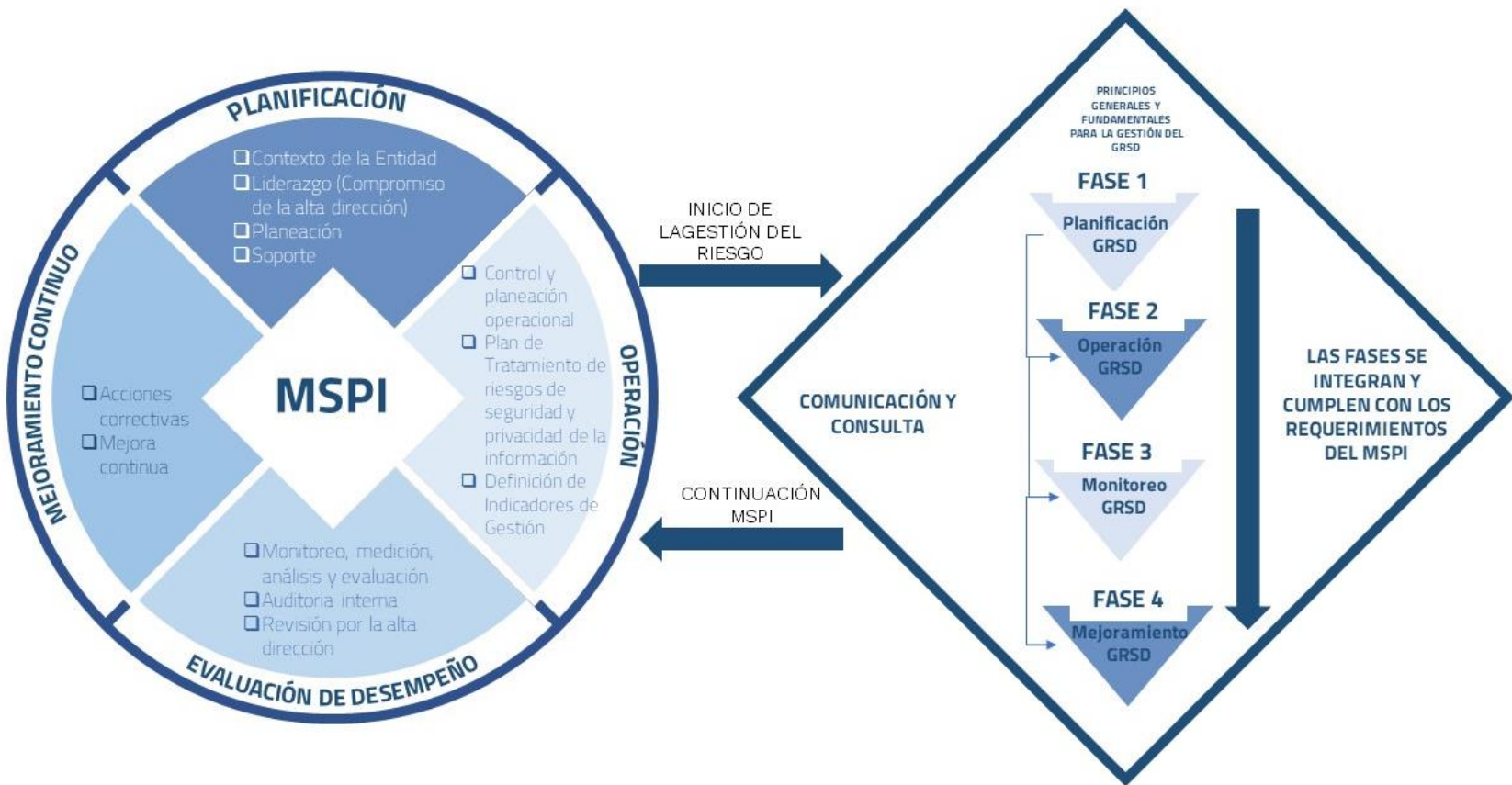
Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, las entidades públicas deben realizar la implementación del **Modelo de Seguridad y Privacidad de la Información (MSPI)** con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información al interior de la Entidad.

El **MSPI** integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el presente Anexo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el **MSPI**.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de **PLANIFICACIÓN** del **MSPI**.
2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de **IMPLEMENTACIÓN** del **MSPI**.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de **EVALUACIÓN DEL DESEMPEÑO** del **MSPI**.
4. Las actividades de **MEJORAMIENTO CONTINUO** en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

A continuación se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información:



FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

3 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA ENTIDADES PÚBLICAS

En los siguientes numerales se indican los aspectos complementarios a lo expuesto en el documento “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*”², donde se incluyen los riesgos de seguridad de la información.

3.1 Fase 1. Planificación de la GRSD

La fase de planificación comprende todo lo expuesto en los **Pasos 1, 2 y 3** de la “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*”, emitida por la Función Pública, es decir, comprende todo lo relacionado con las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos de información.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

Respecto a estas actividades, el presente documento busca profundizar en lo concerniente a riesgos de seguridad de la información, en cada una de ellas, siendo el documento del Departamento administrativo de la Función Pública -DAFP-, el documento metodológico principal.

²La guía para la Administración del Riesgo en la [Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas](#), la encuentra en el portal del Departamento Administrativo de la Función Pública - DAFP.

3.1.1 Contexto interno y externo de la entidad pública

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la entidad, sin embargo, es necesario profundizar en este análisis relacionado con seguridad de la información, por lo tanto, a continuación, se dan unas directrices adicionales para realizar la actividad adecuadamente.

• Establecimiento del contexto externo

Para determinar el contexto externo, la entidad pública debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

CONTEXTO EXTERNO

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad de la información, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

• Establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Para determinar los factores de la entidad pública y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
<ul style="list-style-type: none">• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros• Flujos de información y los procesos de toma de decisiones• Empleados, contratistas	<ul style="list-style-type: none">• Identificación de los procesos y su respectiva caracterización• Detalle de las actividades que se llevan a cabo en el proceso• Flujos de información

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
<ul style="list-style-type: none"> Objetivos estratégicos y la forma de alcanzarlos La misión, visión, valores y cultura de la organización Sus políticas, procesos y procedimientos Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) Toda la estructura organizacional Roles y responsabilidades Sistemas de información o servicios. 	<ul style="list-style-type: none"> Identificación y actualización de los activos en la cadena de valor de la entidad pública Recursos Alcance del proceso Relaciones con otros procesos de la entidad pública Cantidad de ciudadanos afectados por el proceso Procesos de gestión de riesgos que se tienen actualmente implementados Personal involucrado en la toma de decisiones

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Para llevar a cabo esta actividad se sugiere hacer una lista en la que estén enumeradas las partes interesadas externas e internas que tengan relación con la entidad pública y con sus objetivos, misión o visión.

3.1.2 Alcance para aplicar la gestión de riesgos de seguridad de la información

El alcance de la administración del riesgo de seguridad de la información debe ser extensible y aplicable a los **procesos** de la entidad pública que indiquen los criterios diferenciales del **Modelo de Seguridad y Privacidad de la Información**³, habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

3.1.3 Alineación o creación de la política de gestión de riesgo de seguridad de la información.

Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los **riesgos de seguridad de la información** en todos sus niveles. Esta debe crearse como lo indica la *Guía de administración del riesgo de gestión* del DAFP en el **Paso 1**, incluyendo la gestión de riesgos de seguridad de la información. Esta actividad es responsabilidad de la **Línea estratégica** dispuesta por el MIPG.

3.1.4 Definición de roles y responsabilidades

Además de las líneas de defensa y las responsabilidades designadas en la “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*” del DAFP, es necesario indicar o profundizar en las responsabilidades que deberá tener designadas el Responsable de Seguridad digital:

Responsable de Seguridad Digital

Cada entidad pública **debe designar un responsable de Seguridad Digital** que también es el responsable de la **Seguridad de la Información**, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica, como lo establece el Manual Operativo del MIPG en el numeral 3.2.1.4 Política de Seguridad de la

³ http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

información, las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad de la información serán las siguientes:

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Actuar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Nota: Como complemento de esta actividad, la entidad pública debe tomar como referencia lo definido en la **Guía Roles y responsabilidades del MSPI**⁴ de la Estrategia de Gobierno Digital del MINTIC, en complemento a lo anterior.

3.1.5 Definición de recursos para la Gestión de riesgos de seguridad de la información

La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la Entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la Entidad.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

3.1.6 Identificación de activos de información

Un activo de información, es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

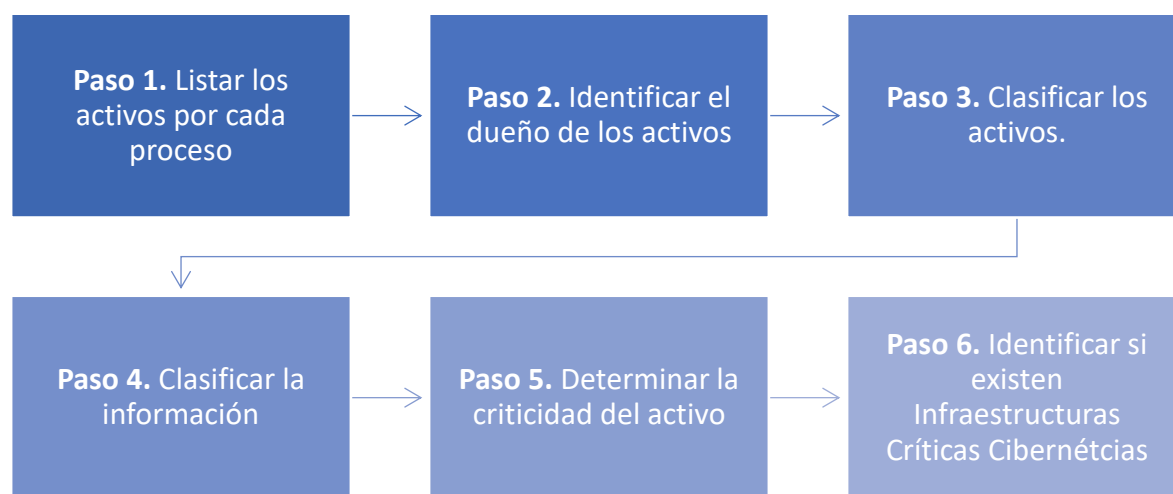
Es necesario que la entidad pública identifique los activos de información y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

⁴ <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html> Guía Roles y Responsabilidades

La identificación y valoración de activos debe ser realizada por la **Primera Línea de Defensa – Líderes de Proceso**, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:

IMAGEN 2. PASOS PARA LA IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS.



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

A continuación, se especifica lo que deberá tenerse en cuenta para la realización de cada uno de los pasos mencionados para la identificación y valoración de activos.

Paso 1. Listar los activos por cada proceso:

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Ejemplo:

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Las entidades públicas pueden adicionar identificadores o nemónicos para complementar la identificación de los activos.

Paso 2. Identificar el dueño de los activos:

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Ejemplo:

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Jefe Oficina de Nómina
Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Generalmente el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

Paso 3. Clasificar los activos:

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware,

La siguiente tabla presenta una propuesta de tipología de activos con el fin de hacer la clasificación mencionada.

TABLA 1. TIPOLOGÍA DE ACTIVOS

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades

Tipo de activo	Descripción
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el 'good will', entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Ejemplo:

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Ejemplo:

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Base de datos de nómina	Información	Información Reservada	No Contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Factura de venta	Información	Información Pública	No contiene datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Al realizar la identificación del contexto externo, la entidad pública debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios para tener en cuenta respecto a la información. El **área jurídica** de la entidad debe colaborar en esta tarea específica.

Paso 5. Determinar la criticidad del activo (Valoración del Activo):

Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia la *Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información* (MSPI)⁵, estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a su completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	software	BAJA	MEDIA	BAJA	MEDIA
Listas de asistencia	Información	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la **Línea Estratégica – Alta dirección**.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICC-

Se invita a que las entidades públicas identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

⁵ <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html> - Guía Gestión Clasificación de Activos

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	\$464.619.736	3 años en recuperación

Fuente: Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia.
Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición.

Si la entidad pública determina que tiene ICC, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

Con base a los seis (6) pasos vistos previamente, la entidad pública podría generar un formato como el siguiente (**ejemplo de referencia**) para generar tanto su procedimiento de identificación e inventario de activos como el formato para hacer su levantamiento. El formato puede variar en cada entidad según la necesidad y normatividad aplicable o si desea integrar otra información.

Proceso	Activo	Descripción	Dueño del Activo	Tipo de Activo	Clasificación de información (Ley 1581 de 2012 / Ley 1712 de 2014)	Criticidad del Activo (Adicionar las preguntas para determinarla)
Ver Paso 1	Ver Paso 1	Ver Paso 1	Ver Paso 2	Ver Paso 3	Ver Paso 4	Ver Paso 5
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe oficina de nómina	Información	Ley 1712 Información reservada Ley 1581 Contiene datos personales Otras normas que apliquen	ALTA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Recomendaciones adicionales para la identificación de activos:

Para identificar los activos, realizar su inventario y clasificación, las entidades públicas pueden emplear los siguientes métodos:

- Revisión de los flujos o diagramas del proceso.
- Revisión de inventarios de activos previos o de otras áreas.
- Entrevistas o lluvia de ideas dentro de cada proceso.

- **Nota:** adicional a lo anterior, la **Guía para la gestión y clasificación de activos del Modelo de Seguridad y Privacidad de la Información** de la Estrategia Gobierno Digital de MINTIC, capítulo 7, también brinda una orientación para clasificar los activos de información.

Importante:

La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el **Modelo de Seguridad y Privacidad de la Información**. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

3.1.7 Identificar los riesgos inherentes de seguridad de la información

Como lo indica el **Paso 2** de la “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*” emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D), fortuitas (F) o ambientales (A).

TABLA 2. TABLA DE AMENAZAS COMUNES

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A

TIPO	AMENAZA	ORIGEN
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Pérdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

FUENTE: ISO/IEC 27005:2009

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

TABLA 3. TABLA DE AMENAZAS DIRIGIDA POR EL HOMBRE

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	<ul style="list-style-type: none"> • Reto • Ego • Rebelión • Estatus • Dinero 	<ul style="list-style-type: none"> • Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	<ul style="list-style-type: none"> • Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos 	<ul style="list-style-type: none"> • Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	<ul style="list-style-type: none"> • Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación 	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Ventaja competitiva • Espionaje económico 	<ul style="list-style-type: none"> • 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,	<ul style="list-style-type: none"> • Curiosidad • Ego • Inteligencia • Ganancia monetaria 	<ul style="list-style-type: none"> • Asalto a un empleado • Chantaje

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
negligentes, deshonestos o despedidos)	<ul style="list-style-type: none"> • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación) 	<ul style="list-style-type: none"> • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

FUENTE: ISO/IEC 27005:2009

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

TABLA 4. TABLA DE VULNERABILIDADES COMUNES

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso

Tipo	Vulnerabilidades
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

FUENTE: ISO/IEC 27005

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza **puede** no requerir la implementación de un control.

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

TABLA 5. TABLA DE AMENAZAS Y VULNERABILIDADES

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Dstrucción 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 física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
	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
SOFTWARE	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

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
RED	Ausencia de mecanismos de identificación y autenticación, como la autenticación 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
	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
RED	Ausencia de identificación y autenticación 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	Dstrucción de equipos y medios

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
LUGAR	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
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
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 auditorías	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 administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	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

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	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: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Identificación del riesgo inherente de seguridad de la información:

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el **dueño del riesgo**, es decir, “quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo”⁶.

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.
- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad de la información se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración
- **Análisis de escenarios:** en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.
- **Otras técnicas que pueden ser empleadas son:** entrevistas estructuradas, encuestas o listas de chequeo.

⁶ GTC 137 Gestión del Riesgo. Vocabulario

Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el **Paso 3. Valoración del Riesgo, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas”** del DAFP.

3.1.8 Identificación del nivel de confianza para la autenticación digital

Se deben identificar aquellos tramites y servicios ciudadanos digitales que deben contar con autenticación digital de acuerdo con lo señalado en la guía de lineamientos para los Servicios Ciudadanos Digitales, en la que se establece que inicialmente, para el acceso al servicio de Autenticación Digital, las entidades deben identificar y determinar el grado de confianza requerido para los procesos relacionados con el trámite acorde con la siguiente clasificación:

Bajo: Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea es mínimo.

Medio: Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea es moderado.

Alto: Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea implica un riesgo alto.

Muy alto: Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea implica un riesgo extremo.

Para la definición del nivel de confianza y establecer el nivel de garantía requerido para el sistema de información asociado al trámite que usará el servicio de Autenticación Digital, se debe realizar el proceso para la valoración de riesgos de Seguridad de la información, señalado en la Guía para la administración de riesgos y diseño de controles de la Función Pública, en el capítulo 5. Lineamientos riesgos de seguridad de la información.

En este sentido es necesario identificar dentro del inventario de activos de información, aquellos activos de tipo software que requieran autenticación digital e identificar si estos trámites y/o servicios digitales solo los puede realizar el titular de la información en cuyo caso es necesario establecer un control de autenticación digital, para identificar el nivel adecuado se debe realizar el análisis de pérdida de confidencialidad, pérdida de integridad y pérdida de disponibilidad, teniendo en cuenta la vulnerabilidad de: Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario; y la amenaza: Falsificación de derechos, sobre estos activos de software (tramites y/o servicios digitales).

Posteriormente se debe realizar el análisis de probabilidad e impacto de la materialización de estos riesgos, para determinar su nivel de riesgo, de acuerdo con los niveles definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. (extremo, alto, moderado o bajo) y así establecer el grado de confianza de autenticación digital adecuados mencionados anteriormente (Muy alto, alto, medio o bajo), una vez identificado el nivel de confianza adecuado se deben seguir los lineamientos de la guía para la vinculación y uso de los servicios ciudadanos digitales, con el fin de realizar el proceso de vinculación al servicio de autenticación digital.

3.1.9 Identificación y evaluación de los controles existentes

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección **4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA** (Tomados del Anexo A de la Norma ISO/IEC 27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad de la información que están enunciados en dicho anexo.

3.1.10 Tratamiento de los riesgos de seguridad de la información

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*” del DAFP: **Evitar, aceptar, compartir o mitigar el riesgo.**

Importante:

Si la entidad pública decide **mitigar o tratar el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la **Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA**, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

3.1.11 Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el **Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos**, de la “*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*” emitida por el DAFP.

3.2 Fase 2. Ejecución

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la **Fase 1**.

Aquí la **Línea Estratégica** debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (**Primer Línea de Defensa** y la **Oficina de Tecnologías de la Información -TI-** generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

3.3 Fase 3. Monitoreo y revisión

La entidad pública a través de las **Tres Líneas de defensa** definidas en el MIPG en la Dimensión 7 Control Interno, Componente **Actividades de control**, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota: una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad de la información que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

3.3.1 Registro y reporte de incidentes de seguridad de la información

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Nota: El reporte de incidentes de seguridad de la información a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre otros), **no es la misionalidad del presente documento**, sin embargo, se recomienda realizar dichos reportes conforme lo estipulan los entes o las buenas prácticas en seguridad de la información.

3.3.2 Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

REPORTE

1. Listado de los riesgos identificados de seguridad de la información.
2. Listado de activos críticos TI/TO y listado de ICC.
3. Reporte de criticidad/impacto de la organización.
4. Plan de tratamiento de riesgos.
5. Reporte de evolución de riesgos y modificación del riesgo.
6. Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
7. Impacto económico que podría presentarse frente a la materialización de los riesgos.

PERIODICIDAD

- > Periódicamente por parte de todas las Entidades u organizaciones que han adoptado el modelo respectivo.
- > Cuando ocurra un cambio organizacional o de procesos de la organización que genere un impacto en las operaciones o que pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de los riesgos y reportar los resultados a la Entidad de control.
- > Cuando se incluya un nuevo proceso dentro del alcance de la gestión de riesgos de seguridad de la información de la Entidad. En este caso se debe realizar una nueva evaluación de riesgos y reportar los resultados a la Entidad de control.

IMAGEN 3. REPORTES DE INFORMACIÓN POR PARTE DE LA ENTIDAD.

FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

3.3.3 *Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales*

Una vez la entidad pública obtenga los resultados de la gestión de riesgos de seguridad de la información, se debería consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el Gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad de la información.

Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet)
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad de la información de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:

Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deberían reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional.

Nota: Es importante indicar que los reportes de riesgos de seguridad de la información a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

3.3.4 Auditorías internas y externas

Le corresponde a las **Unidades de Control Interno (tercera línea de defensa)**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad de la información en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

3.3.5 Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores⁷) para la gestión de los riesgos de seguridad de la información, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

3.4 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad de la información

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad de la información, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

⁷ Consultar en la *Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad de la información* del DAFP – Sección Indicadores - Gestión del Riesgo de Seguridad de la información, para definir indicadores de seguimiento para la gestión del riesgo de seguridad de la información.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Empezar acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

4 CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando los controles, del **numeral 12.1 Controles y objetivos de control**, del documento maestro del Modelo de Seguridad y Privacidad de la Información – MSPI.