GUÍA DE ORIENTACIÓN PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN EL **GOBIERNO NACIONAL, TERRITORIALES Y SECTOR PÚBLICO**

Tabla de contenido

Tabla de imágenes **4**

Índice de tablas **5**

Introducción **6**

1. Generalidades **8**

1.1 Derechos de autor *8*

1.2 Audiencia *9*

1.3 Objetivos *10*

1.3.1 Objetivo general 10

1.3.2 Objetivos específicos 10

1.4 Alcance de la guía *10*

1.5 Glosario *10*

2. Justificación **11**

3. Interacción del modelo de seguridad de la información (MSPI) con el modelo nacional de gestión de riesgos de seguridad digital (MGRSD) **12**

4. Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público **14**

4.1 Fase 1. Planificación de la GRSD *14*

4.1.1 Compromiso de la alta dirección 14

4.1.2 Contexto de la entidad 14

4.1.3 Identificación de las múltiples partes interesadas con la GRSD 17

4.1.4 Identificación de procesos donde se aplique la gestión de riesgos de seguridad digital 18

4.1.5 Asociación de la política de gestión de riesgo de seguridad digital con políticas existentes 20

4.1.6 Definición de roles y responsabilidades 21

4.1.7 Definición de recursos para la GRSD 23

4.1.8 Establecimiento de criterios para evaluación de los riesgos de seguridad digital 23

4.2 Fase 2. Ejecución de la GRSD 30

4.2.1 Identificación de activos de información 30

4.2.2 Identificar los riesgos inherentes de seguridad digital 35

4.2.3 Valoración de riesgos inherentes de seguridad digital 40

4.2.4 Identificación y evaluación de los controles 44

4.2.5 Tratamiento de los riesgos de seguridad digital 50

4.3 Fase 3. Monitoreo y revisión 53

4.3.1 Registro y reporte de eventos de riesgos de seguridad digital 53

4.3.2 Auditorías internas y externas 56

4.3.3 Revisión por parte de la alta dirección 56

4.3.4 Medición del desempeño 56

4.3.5 Rendición de cuentas 56

4.4 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad digital 57

4.4.1 Comunicación y consulta 58

Tabla de imágenes

Imagen 1. Interacción entre el MSPI y el MGRSD. Fuente: MinTIC 12

Imagen 2. Mapa de calor. Fuente: elaborado por el autor 29

Imagen 3. Mapa de calor con definición del apetito de riesgo. Fuente: elaborado por el autor 30

Imagen 4. Ejemplo determinación probabilidad de ocurrencia e impacto. Fuente: elaborado por el autor 43

Imagen 5. Determinación del riesgo residual. Fuente: elaborado por el autor..... 50

Imagen 6. Reporte de información por parte de la entidad. Fuente: MinTIC 54

Índice de tablas

Tabla 1. Criterios de valoración de impacto de acuerdo con la información 25

Tabla 2. Criterios de valoración de la probabilidad de ocurrencia 27

Tabla 3. Zona de riesgos de acuerdo con la combinación de impacto y probabilidad 28

Tabla 4. Ejemplo de clasificación de activos 32

Tabla 5. Ejemplo de preguntas para determinar el nivel de importancia de los activos 33

Tabla 6. Clasificación de la información 34

Tabla 7. Tabla de amenazas comunes 36

Tabla 8. Tabla de amenazas dirigida por el hombre 37

Tabla 9.Ejemplos de vulnerabilidades y amenazas 38

Tabla 10. Ejemplos de riesgos asociados a las amenazas y vulnerabilidades 39

Tabla 11. Ejemplo valoración del riesgo inherente de seguridad digital 42

Tabla 12. Cualidades de los controles 44

Tabla 13. Características de los controles 45

Tabla 14. Análisis y evaluación de controles 47

Tabla 15. Rango de calificación de los controles 47

Tabla 16. Ejemplos de planes de acción para el tratamiento de riesgos 52

Tabla 17. Ejemplo de una matriz de comunicación 58

Introducción

La globalización de las tecnologías de la información y las comunicaciones se ha multiplicado en los últimos años; por consiguiente, el desarrollo de las comunicaciones ha crecido a tal punto que el mundo está interconectado casi por completo. Lo anterior impulsa a los sectores estratégicos a comunicarse a través de infraestructuras operativas, dispositivos de tecnología fija, inalámbrica o móvil, lo que genera un incremento en la información transferida, dependencias con otros sistemas de información y manipulación por diferentes actores.

Es evidente que la interoperabilidad y el crecimiento de las redes de comunicaciones, sin un debido control o gestión de los riesgos, expongan la información a un sinnúmero de amenazas y de vulnerabilidades que afectan, no solo la infraestructura tecnológica, sino la información almacenada o transferida a través de ellas. Por lo tanto, se hace necesaria la implementación de un sistema de gestión de riesgos que permita proteger la información sensible y estratégica, la infraestructura tecnológica y las infraestructuras críticas cibernéticas (ICC) de la nación.

El Ministerio de las TIC (MinTIC) busca fortalecer los lineamientos definidos en el documento CONPES 3854 con la creación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD). En este modelo los gestores de los sistemas de información, comunicaciones o servicios informáticos, entre otros, que tengan relación con la información del país, son actores principales que deben ser conscientes de los riesgos presentes en el entorno digital y de las medidas correctivas que deben implementarse para fortalecer la seguridad de la información en cada una de las entidades. Esto contribuye con el desarrollo social, económico y ambiental del país.

Lo anterior sugiere que la nación, a través de las entidades públicas, puede gestionar los riesgos asociados al entorno digital y aumentar la eficiencia, la

confianza y la seguridad en la prestación de los servicios a los ciudadanos, como también contribuir, a su vez, a la continuidad del gobierno digital.

De acuerdo con lo anterior, y como extensión del MGRSD, se establece esta guía como herramienta para implementar las mejores prácticas para la gestión de riesgos de seguridad digital en las entidades gubernamentales, territoriales y públicas.

Para su aplicación, se ha considerado la importancia que tiene la información de estas entidades dentro de su entorno digital y también aquellas que sean consideradas infraestructuras críticas cibernéticas[1] en su mismo ámbito.

Esta guía se encuentra enmarcada en los principios fundamentales y generales del riesgo de seguridad digital, donde se ha establecido la etapa de comunicación y consulta de forma transversal a todas las fases de la metodología. De igual forma, la guía está soportada en el denominado ciclo PHVA (planear, hacer, verificar y actuar)[2], lo que permite que la entidad pueda adaptarla e integrarla con otros sistemas de gestión que tenga implementados en la actualidad.

Finalmente, esta guía hace parte de las herramientas del modelo integrado de planeación y gestión (MIPG) en desarrollo del decreto 1499 de 2017, donde se busca una gestión del riesgo integral como se habla en la dimensión de direccionamiento estratégico y planeación.

---

[1] Glosario, modelo nacional para la gestión de riesgos digitales numeral 4.

[2] Ciclo PHVA conocido como el Ciclo Deming por su asociación con su autor Edward Deming.

1. Generalidades

1.1 Derechos de autor

Todas las referencias a los documentos del modelo nacional de gestión de riesgos de seguridad digital, 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 Ministerio de Tecnologías de la Información y las Comunicaciones, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del Modelo Nacional de gestión de riesgos de seguridad digital publicadas en el compendio de las normas técnicas colombianas vigentes.

En consecuencia, el Ministerio de Tecnologías de la Información y las Comunicaciones goza de los derechos de autor[3] establecidos en la ley 23 de 1982

[3] **Ley 1520 de 2012. Artículo 5.** El artículo 12 de la ley 23 de 1982 dice: "**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 queda así: "Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimento 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 puede intentar directamente o por intermedia persona acciones

y demás normas concordantes y complementarias, respecto de los documentos del Modelo Nacional de Gestión de Riesgos de Seguridad Digital y su contenido.

Las reproducciones, referencias o enunciaciones de estos Documentos deben 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 modelo nacional de gestión de riesgos de seguridad digital y sus documentos o anexos que son de su autoría o propiedad.

1.2 Audiencia

Esta guía está dirigida para la aplicación en las entidades del Gobierno nacional, territoriales y sector público, así como proveedores de servicios de Gobierno en línea, de acuerdo con lo establecido por el Departamento Administrativo de la Función Pública (DAFP) en el Manual de estructura del Estado colombiano.[4]

---

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.

[4] Manual de estructura del Estado colombiano: http://www.funcionpublica.gov.co/eva/es/biblioteca-virtual/manual-del-estado-colombiano/manualestructuraestadocolombiano

1.3 Objetivos

1.3.1 Objetivo general

El objetivo principal de esta guía es orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del MGRSD para, entre otros aspectos, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad.

1.3.2 Objetivos específicos

a. Otorgar una herramienta para la ejecución de la GRSD en las entidades de Gobierno, territoriales y del sector público en general.
b. Estandarizar el proceso de gestión de riesgos de seguridad digital en las entidades del Gobierno, territoriales y del sector público en general.
c. Generar mecanismos para que las entidades 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.

1.4 Alcance de la guía

Está definido para que su aplicación se realice en las entidades del Gobierno colombiano, entes territoriales y sector público en general.

1.5 Glosario

Ver Glosario en el numeral 4 del modelo nacional de gestión de riesgos de seguridad digital (MGRSD).

2. Justificación

El Gobierno nacional ha desarrollado mayor conciencia sobre las amenazas existentes en el entorno digital colombiano. Por eso, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) busca orientar a las entidades que forman parte del alcance de esta guía en la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad digital, incluidas las ya mencionadas ICC nacionales. La guía tiene como fin fortalecer el entorno digital, maximizar beneficios sociales y económicos, asegurar la provisión de servicios seguros y confiables, gestionar las infraestructuras críticas cibernéticas, propender por respetar los derechos humanos y los valores fundamentales; así como proteger a la ciudadanía en general frente a los riesgos a los que estaría expuesta en relación con la seguridad digital.

En consecuencia, y después de planteada la necesidad, se crea la guía como parte del modelo nacional de gestión del riesgo de seguridad digital (MGRSD), la cual desarrolla cada una de las fases de implementación de la metodología de gestión de riesgos de seguridad digital para las entidades del Gobierno nacional, territoriales y del sector público.

Antes de iniciar la aplicación de esta guía, es importante que la entidad establezca claramente el grado de madurez frente a los requerimientos de gestión de riesgos de seguridad definidos por el modelo de seguridad y privacidad de la información (MSPI) que hace parte de estrategia de Gobierno en línea. Con base en lo anterior, si la entidad no cuenta con un sistema de gestión que involucre o tenga asociada una metodología de gestión de riesgos, entonces debe tomar como referencia la presente guía, específicamente para los riesgos de seguridad digital. Así mismo, la entidad debe articular la evaluación de los riesgos de seguridad digital con las demás tipologías de riesgos y seguir las prácticas que dispone el departamento de administración de la función pública (DAFP).

3. Interacción del modelo de seguridad de la información (MSPI) con el modelo nacional de gestión de riesgos de seguridad digital (MGRSD)

Conforme lo indica el ámbito de aplicación del decreto 1078 de 2015 respecto a la implementación de la estrategia de Gobierno en línea (GEL), las entidades públicas deben realizar la ejecución del modelo de seguridad y privacidad de la información (MSPI) con el objetivo de conformar un sistema de gestión de seguridad de la información al interior de la entidad. El modelo de seguridad y privacidad de la información (MSPI) cuenta con el componente de gestión de riesgos a través de las etapas de planificación y ejecución, su relación e interacción con el modelo nacional de gestión de riesgos de seguridad digital (MGRSD) se resume a continuación:

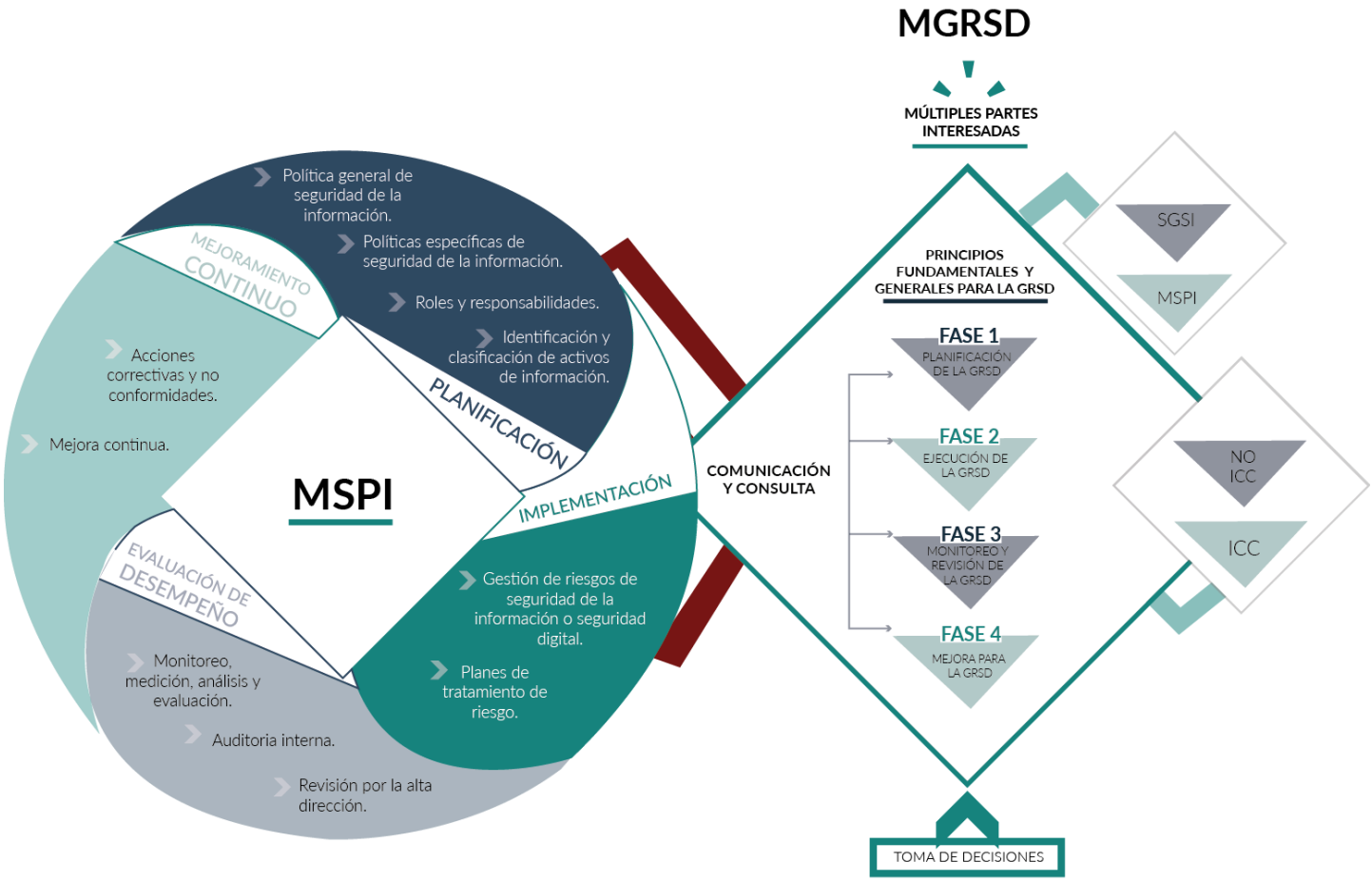

Imagen 1. Interacción entre el MSPI y el MGRSD. Fuente: MinTIC

Es importante aclarar que la gestión de riesgos de seguridad digital (GRSD) contempla las actividades de identificación, análisis, evaluación y tratamiento; Así mismo, todo lo referente al grado de aceptación, al nivel de apetito de riesgo definido por cada entidad y el aseguramiento para llevar a cabo el plan de tratamiento de riesgos respectivo, conforme a los periodos establecidos para tal efecto. Todo esto va relacionado con los aspectos de mejoramiento continuo en la entidad y particularmente, con la seguridad de la información en el MSPI.

Adicionalmente, las entidades también deben aplicar de forma transversal las fases de comunicación y consulta, así como las de monitoreo y revisión del MGRSD, las cuales están relacionadas con la fase de mejora continua del MSPI.

4. Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público

En los siguientes numerales se desarrolla paso a paso el proceso de gestión del riesgo, conforme a lo establecido en el modelo nacional de gestión del riesgo de seguridad digital (MGRSD).

4.1 Fase 1. Planificación de la GRSD

La fase de planificación es el punto de partida para llevar a cabo el proceso de la gestión de riesgos de seguridad digital. Por tanto, es considerada una fase esencial donde se identifica el contexto de la entidad, el ecosistema digital, los criterios de impacto y probabilidad, así como el apetito de riesgo, entre otros parámetros que resultan necesarios para llevar a cabo de buena forma la gestión de riesgos de seguridad digital. De acuerdo con lo anterior, se desarrolla con mayor énfasis la definición de los elementos que la entidad debe precisar durante la etapa de planificación.

4.1.1 Compromiso de la alta dirección

La alta dirección debe brindar un altísimo compromiso para llevar a cabo el proceso de gestión del riesgo de seguridad digital, a través del establecimiento de políticas, objetivos, roles y responsabilidades que aportan los recursos necesarios para que el proceso sea desarrollado de forma efectiva.

4.1.2 Contexto de la entidad

Para la identificación del contexto se deben tener en cuenta los factores internos y externos del entorno digital, en especial aquellos que puedan impactar directamente como son: misión, objetivos y las partes interesadas, en particular y lo que resulte concerniente para la toma de decisiones.

4.1.2.1 Establecimiento del contexto externo

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

- ✓ Grupos de interés externos y partes interesadas (ver numeral 4.1.3 Identificación de partes interesadas).
- ✓ Clientes, proveedores de servicios y empresas que sean competencia directa y se relacionen con la misión de la entidad analizada.
- ✓ Regulaciones, normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014.
- ✓ Dependencias económicas y financieras por parte de otras empresas.
- ✓ Entorno cultural.
- ✓ Cualquier otro factor externo de tipo internacional, nacional, regional o local.
- ✓ Cantidad de ciudadanos a los cuales la entidad brinda servicios a través del entorno digital.
- ✓ Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad.

4.1.2.2 Establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- ✓ La entidad en general, su organización, sistemas de información, 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 y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

Para la entidad

- ✓ Recursos económicos, social, ambiental, físicos, tecnológicos, financieros, jurídicos, entre otros
- ✓ Flujos de información y los procesos de toma de decisiones
- ✓ Partes interesadas internas
- ✓ 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

Para los procesos:

- ✓ Identificación de los procesos y su respectiva caracterización
- ✓ Detalle de las actividades que se llevan a cabo en el proceso
- ✓ Flujos de información
- ✓ Recursos
- ✓ Alcance del proceso
- ✓ Relaciones con otros procesos de la entidad
- ✓ Cantidad de ciudadanos afectados por el proceso
- ✓ Procesos de gestión de riesgos que se tienen actualmente implementados
- ✓ Personal involucrado en la toma de decisiones

4.1.2.3 ¿Quiénes participan en el establecimiento del contexto?

Para llevar a cabo esta actividad, se sugiere realizar sesiones de trabajo donde se involucren los siguientes roles (cuando aplique):

- ✓ Gerentes de áreas
- ✓ Jefes de oficina
- ✓ Líderes de proceso
- ✓ Líderes funcionales
- ✓ Encargados de los sistemas de gestión
- ✓ Encargados de los sistemas de información
- ✓ Personal jurídico
- ✓ Cualquier otro rol que la entidad considere relevante

Para la documentación de esta actividad puede utilizarse cualquier instrumento que la entidad considere necesario y donde se consigne la información recopilada durante las sesiones de trabajo, como son: un documento, una matriz o un flujograma, entre otros.

4.1.3 Identificación de las múltiples partes interesadas con la GRSD

Algunas partes interesadas con la gestión de riesgo de seguridad digital, que podrían evaluarse son:

- ✓ Proveedores de servicio que soportan los procesos tecnológicos de la entidad
- ✓ Entidades que dependen de la generación de información de la propia entidad
- ✓ Cantidad de ciudadanos que gozan de los servicios prestados por la entidad
- ✓ Empresas vinculadas con la entidad
- ✓ Personal: funcionarios públicos, trabajadores oficiales, contratistas y personal de convenios
- ✓ Medios de comunicación

- ✓ Organizaciones nacionales e internacionales
- ✓ Grupos religiosos
- ✓ Gobierno nacional

4.1.3.1 ¿Quiénes participan en la identificación de las partes interesadas?

Para llevar a cabo esta actividad se sugiere realizar sesiones de trabajo donde se involucren los siguientes roles (si aplica):

- ✓ Gerentes de áreas
- ✓ Jefes de oficina
- ✓ Líderes de proceso
- ✓ Líderes funcionales
- ✓ Encargados de los sistemas de gestión
- ✓ Encargados de los sistemas de información
- ✓ Personal jurídico
- ✓ Cualquier otro rol que la entidad considere relevante

Para la documentación de esta actividad puede utilizarse cualquier instrumento que la entidad considere necesario y donde se consigne la información recopilada durante las sesiones de trabajo, como son: un documento, una matriz, entre otros.

4.1.4 Identificación de procesos donde se aplique la gestión de riesgos de seguridad digital

Es fundamental que la entidad, al desarrollar su gestión de riesgos de seguridad digital, cuente con la identificación de los procesos donde aplique la presente guía. Por lo tanto, si no tiene una caracterización de los procesos, entonces podría definirla, sin limitarse, en los siguientes factores:

- ✓ ¿Quién ejecuta el proceso?
- ✓ ¿Quiénes son los beneficiarios?

- ✓ ¿Cuáles son los objetivos?
- ✓ ¿Cuáles son las actividades y flujo de operación?
- ✓ ¿Qué se requiere para ejecutarlo?
- ✓ ¿Cuáles son las entradas y salidas?
- ✓ ¿Cuáles son las partes interesadas?
- ✓ ¿Quiénes son los responsables?
- ✓ ¿Cuáles son los recursos?
- ✓ ¿Qué interacción tiene con otros procesos?
- ✓ Otra información relevante y asociada al proceso

4.1.4.1 ¿Quiénes participan en la identificación de los procesos de la entidad?

Para llevar a cabo esta actividad se sugiere, al igual que los pasos anteriores, realizar una sesión de trabajo donde se involucren los siguientes roles (cuando aplique):

- ✓ Gerentes de áreas
- ✓ Jefes de oficina
- ✓ Líderes de proceso
- ✓ Líderes funcionales
- ✓ Encargados de los sistemas de gestión
- ✓ Encargados de los sistemas de información
- ✓ Personal jurídico
- ✓ Cualquier otro rol que la entidad considere relevante

Para la documentación de esta actividad puede utilizarse cualquier instrumento que la entidad considere necesario y donde se consigne la información recopilada durante las sesiones de trabajo, como son: listas de chequeo, un documento, un flujograma, entre otros.

Nota: para la ejecución de esta labor se debe tener en cuenta lo estipulado en el manual operativo del MIPG, en su sección Operación interna-Procesos institucionales.

4.1.5 Asociación de la política de gestión de riesgo de seguridad digital con políticas existentes

Para la asociación de la política de gestión de riesgo de seguridad digital, la entidad debe tener en cuenta los lineamientos establecidos previamente por el departamento administrativo de función pública, con el fin de que las políticas de gestión de riesgo se armonicen en una sola y se incluya el compromiso de la gestión de los riesgos de seguridad digital[5]. Si esta política no existe, debe crearse como lo indica el manual operativo del MIPG y que contenga la gestión de riesgos de seguridad digital. Esta actividad es responsabilidad de la alta dirección y del comité institucional de coordinación.

4.1.5.1 ¿Cómo establecer o asociar la política de riesgos de seguridad digital?

Cuando existen políticas dentro de la organización: para llevar a cabo esta actividad se recomienda, como primera medida, identificar si se cuenta con la siguiente información:

- ✓ Políticas de gestión de riesgos existentes dentro de la entidad
- ✓ Sistemas de gestión de seguridad de la información que incluya políticas para la gestión de riesgo de seguridad digital

[5]Para la articulación de la política, la entidad puede tomar como referencia la guía 2 del modelo de seguridad de la información "Elaboración de la política general de seguridad y privacidad de la información" MinTIC, estrategia Gobierno en línea (GEL).

- ✓ Políticas de seguridad de la información donde se involucre la gestión de riesgos

Una vez cuente con esta información, es importante entender el alcance de cada una de las políticas, con el fin de relacionarlas y tratar de alinearlas de tal forma que queden establecidas en una política integral como lo indica el manual operativo del MIPG, en donde se evidencia también el compromiso de la entidad frente a la gestión de riesgos de seguridad digital.

Cuando no se cuenta con políticas dentro de la organización: si aún no cuenta con políticas de gestión de riesgo de ningún tipo, se recomienda tomar como referencia el manual operativo del MIPG de la función pública, para la creación de la política integral de gestión de riesgos, donde se incluya la gestión de riesgos de seguridad digital.

4.1.6 Definición de roles y responsabilidades

La entidad debe definir los roles y responsabilidades de cada uno de los integrantes en el desarrollo de la gestión de riesgos de seguridad digital. Es importante tener en cuenta que la GRSD no está limitada a un único responsable, a una sola área o a un solo proceso, sin embargo, se deben establecer personas que coordinen la gestión.

4.1.6.1 ¿Cómo definir los roles y responsabilidades para la GRSD?

Para efectuar la asignación de roles y responsabilidades hay que tener en cuenta:

Si la entidad cuenta con la implementación de cualquier sistema de gestión de riesgos se debe:

- ✓ Tomar como base esta estructura organizacional y articularla con la gestión de riesgos de seguridad digital

- ✓ Asignar una nueva responsabilidad al área o cargo de la implementación y seguimiento de la gestión de los riesgos de seguridad digital
- ✓ Definir al responsable de la seguridad de la información o seguridad digital (que a su vez es el responsable de liderar la ejecución del MSPI)
- ✓ Definir el administrador para los riesgos de seguridad digital, el cual realice el seguimiento y control de:
  - La ejecución del presupuesto asignado para la GRSD
  - Los recursos humanos destinados para tal efecto
  - Las herramientas que se determinen para la aplicación de los controles
  - En general, todo lo asociado a los proyectos estratégicos donde se registre evidencia del desarrollo de esta actividad

Si la entidad no cuenta con un sistema de gestión de riesgos, la alta dirección debe:

- ✓ Adquirir un compromiso con la implementación y seguimiento a la gestión de riesgos de seguridad digital
- ✓ Designar el área o cargo para la ejecución y seguimiento de la gestión de los riesgos de seguridad digital
- ✓ Definir el administrador para los riesgos de seguridad digital, el cual realice el seguimiento y control de:
  - La ejecución del presupuesto asignado para la GRSD
  - Los recursos humanos destinados para tal efecto
  - Las herramientas que se determinen para la aplicación de los controles
  - En general, todo lo asociado a los proyectos estratégicos donde se registre evidencia del desarrollo de esta actividad

Estos roles se definen y asignan dependiendo de la naturaleza y misión de la entidad, los recursos disponibles, las competencias del personal involucrado o el nivel de interacción con los procesos donde se realiza la gestión de riesgo de seguridad digital.

Nota: como complemento de esta actividad, la entidad puede tomar como referencia lo definido por la guía número 4 Roles y responsabilidades del MSPI de la estrategia Gobierno en Línea (GEL) del MinTIC.

4.1.7 Definición de recursos para la GRSD

La organización debe disponer de los recursos suficientes para el desarrollo de la GRSD, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de ayudar a los responsables en la implementación y seguimiento de los riesgos de seguridad digital.

4.1.7.1 ¿Cómo realizar la definición de los recursos?

La alta dirección debe asignar los recursos adecuados para la gestión del riesgo tales como:

- ✓ Recursos necesarios para cada paso del proceso de gestión de riesgos de seguridad digital
- ✓ Personal capacitado e idóneo para la gestión de riesgo entre los cuales pueden estar los estratégicos tácticos y operativos
- ✓ Recursos económicos para formar las competencias del personal para la implementación de controles de mitigación de riesgos aspectos de mejora continua monitoreo y auditorías

4.1.8 Establecimiento de criterios para evaluación de los riesgos de seguridad digital

La entidad debe establecer los criterios que se definan en los diferentes niveles para valorar los riesgos de seguridad digital en el marco de:

- ✓ La probabilidad y el impacto asociados al riesgo en cuestión
- ✓ Las cualidades y las características de los controles que estén asociados a los riesgos de seguridad digital

- ✓ El nivel de aceptación o apetito del riesgo de seguridad digital
- ✓ Las zonas con su respectiva definición, donde se ubiquen los riesgos inherentes durante el análisis y los riesgos residuales durante su evaluación y posterior tratamiento

La entidad debe definir escalas o niveles de medición de los riesgos de seguridad digital, ya sea de forma autónoma o basada en metodologías adoptadas previamente. Por ejemplo, para criterios de impacto y de probabilidad, puede definir escalas de tres, cuatro, cinco, seis o siete niveles, no hay escalas obligatorias, sin embargo, para efectos de esta guía, se propone la definición de una escala de medición para el impacto, probabilidad y riesgo de seguridad digital de cinco niveles, de acuerdo con lo propuesto por la guía para la administración del riesgo de la función pública[6].

En caso de que la entidad no cuente con un alto grado de madurez para la medición de los riesgos, se deben establecer criterios netamente cualitativos y posteriormente de manera semicuantitativa, y para algunas consideraciones de forma cuantitativa.

4.1.8.1 Definición de los criterios de impacto

Basado en el contexto en el cual se establece el MGRSD, las variables a considerar, para definir los criterios de impacto, son: integridad (I), disponibilidad (D) confidencialidad (C), social (S), económica (E), ambiental (A), las cuales se exponen a continuación:

[6] Guía para la administración del riesgo de la función pública pág. 19 y 20, https://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADa+de+Riesgos+y+Caja+de+Herramientas.rar/a125ddf9-8a7b-4615-860c-2c63c38ad74a

Tabla 1. Criterios de valoración de impacto de acuerdo con la información

Nivel asignado	Valor del impacto	Criterios de impacto para características de seguridad de la información					
		Integridad (I)	**Disponibilidad (D)**	**Confidencialidad (C)**	**Social (S)**	**Económica (E)**	**Ambiental (A)**
Insignificante	1	Sin afectación de la integridad	Sin afectación de la disponibilidad	Sin afectación de la confidencialidad	Afectación del X % de la población o menos	Afectación del X % del presupuesto anual de la entidad o menos	Sin Afectación medioambiental
Menor	2	Afectación muy leve de la integridad	Afectación muy leve de la disponibilidad	Afectación muy leve de la confidencialidad	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación leve del MA requiere de X meses de recuperación
Moderado	3	Afectación leve de la integridad de la información debido al interés particular de los empleados y terceros	Afectación leve de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación leve de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación leve del MA requiere de X años de recuperación
Mayor	4	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación importante del MA que requiere de X años de recuperación
Catastrófico	5	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación muy grave del MA que requiere de X años de recuperación

Fuente: estrategia de Gobierno en línea (GEL) dentro del marco del MSPI

Como sugerencia para la aplicación de la presente guía, la organización debe tener en cuenta lo siguiente:

- ✓ Las variables de *integridad, disponibilidad y confidencialidad* se definen de acuerdo con la estrategia de Gobierno en línea (GEL).[7]
- ✓ La variable *población* se define teniendo en cuenta el establecimiento del contexto externo de la entidad (numeral 4.1.2.1), sobre el cual se está desarrollando el ejercicio, ya sea por la entidad de Gobierno, ente territorial o del sector público. Esto significa que para la variable *social,* la consideración de *población* va a estar asociada a las personas a las cuales se les prestan servicios a través del entorno digital, y que de una forma u otra pueden verse afectadas por la materialización de algún riesgo, los porcentajes en las escalas pueden variar, según el tamaño de la población afectada.
- ✓ Para la variable *económica,* la consideración de *presupuesto* es la más acertada en el sentido del alcance de esta guía, dado que la gran mayoría de las entidades que la empleen dependen principalmente de la asignación del presupuesto que hacen en los municipios las gobernaciones o el Gobierno central para el desarrollo normal de las actividades propias de cada una de ellas.
- ✓ Para la variable *ambiental*, la consideración estará también alineada con la consideración de la *afectación del entorno* por la materialización de un riesgo de seguridad digital.

Nota: en esta consideración es importante establecer que los criterios que se están sugiriendo corresponden a un modelo semicuantitativo de evaluación de los impactos, dada la utilización de variables económicas que permiten estimar de buena forma, unas instancias más cercanas a la realidad de cada entidad. Es de

[7] Guía para la gestión y clasificación de activos de información págs. 16, 17 y 18.

anotar que para aquellas que ya tengan un grado de madurez en el sistema de gestión de riesgos digitales y deseen aplicar una medición cuantitativa, pueden tomar como referencia el Método de simulación Montecarlo, árbol de decisiones, sumas estadísticas, PERT y *Hazard and Operability Study* (Hazop), entre otros.

4.1.8.2 Definición de criterios de probabilidad

Para la definición de escalas o criterios de probabilidad se debe tomar como referencia la metodología de riesgos del DAFP y en general las buenas prácticas de riesgos que se sugieren una escala de cinco niveles como se muestra a continuación:

Tabla 2. Criterios de valoración de la probabilidad de ocurrencia

Criterios de valoración de la probabilidad de ocurrencia			
Nivel asignado	**Valor de la probabilidad**	**Frecuencia del evento**	**Posibilidad de ocurrencia del evento**
Raro	1	La situación se ha presentado al menos cada diez años	La situación puede suceder al menos cada diez años
Improbable	2	La situación se ha presentado al menos una vez cada año	La situación puede suceder al menos una vez cada año
Posible	3	La situación se ha presentado al menos una vez cada semestre	La situación puede suceder al menos una vez cada semestre
Probable	4	La situación se ha presentado al menos una vez al mes	La situación puede suceder al menos una vez al mes
Casi seguro	5	La situación se ha presentado al menos una vez a la semana	La situación puede suceder al menos una vez a la semana

Fuente: elaborado por el autor

4.1.8.3 Definición del nivel o zona de riesgo

La combinación de impacto y probabilidad estará representada por unos intervalos de valor y una descripción que establece a su vez una representación gráfica lo que se ha denominado en el contexto de la gestión de riesgos, “mapa de calor”.

Zona de riesgo: las zonas de riesgo que se consideran para esta guía, y según lo dispuesto por el DAFP, en los cinco niveles de impacto y en los cinco niveles de probabilidad (donde veinticinco es el mayor valor) son los siguientes:

Tabla 3. Zona de riesgos de acuerdo con la combinación de impacto y probabilidad

Zona de riesgo	Valor asignado	Acción requerida
Extremo	Mayor o igual a 15 y hasta 25	Requiere acciones inmediatas para evitar la materialización de los riesgos asociados a la seguridad digital
Alto	Mayor o igual a 9 y menor de 15	Requiere acciones rápidas, a corto plazo, por parte de la alta dirección para disminuir los riesgos asociados a la seguridad digital
Moderado	Mayor o igual a 4 y menor de 9	Requiere medidas a mediano plazo y adecuadas, que permitan disminuir los riesgos asociados a la seguridad digital
Bajo	Menor de 3	Requiere monitoreo y seguimiento a través de actividades propias de la entidad y preferiblemente de acciones de detección y prevención

Fuente: elaborado por el autor

Valor asignado: el valor asignado se refiere a los valores sobre los que se establece la combinación del impacto y la probabilidad de un riesgo identificado. Por ejemplo, si el valor del impacto de un riesgo (analizadas las variables de confidencialidad, integridad, disponibilidad, social, ambiental o económica) es igual a cuatro y el valor de la probabilidad es dos el nivel de riesgo es igual a ocho, lo que lo ubica en la zona de riesgo moderado.

Acción requerida: se refiere a que los riesgos que caigan en la zona de riesgo correspondiente, deben tomar las alternativas sugeridas.

No obstante, las zonas, al igual que los niveles de impacto y probabilidad, se establecen según la necesidad de la entidad que esté aplicando el modelo de gestión de riesgos de seguridad digital (MGRSD).

Estas zonas se van a visualizar en un mapa de calor, como se determina en el contexto de la gestión de riesgos a nivel general.

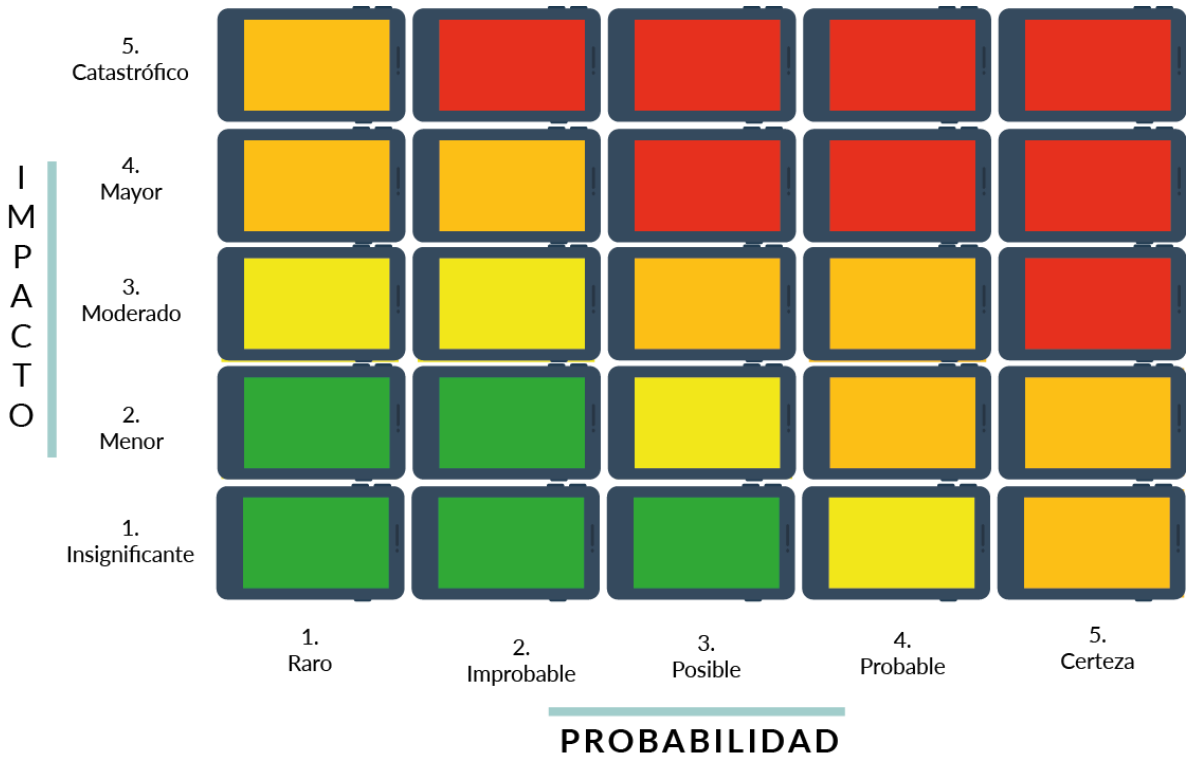

Imagen 2. Mapa de calor. Fuente: elaborado por el autor

4.1.8.3 Definición de apetito o zona de aceptación del riesgo

Es el máximo nivel de riesgo que la organización está dispuesta aceptar. En la siguiente imagen se presenta en línea punteada la definición del apetito de riesgo que una entidad puede definir.

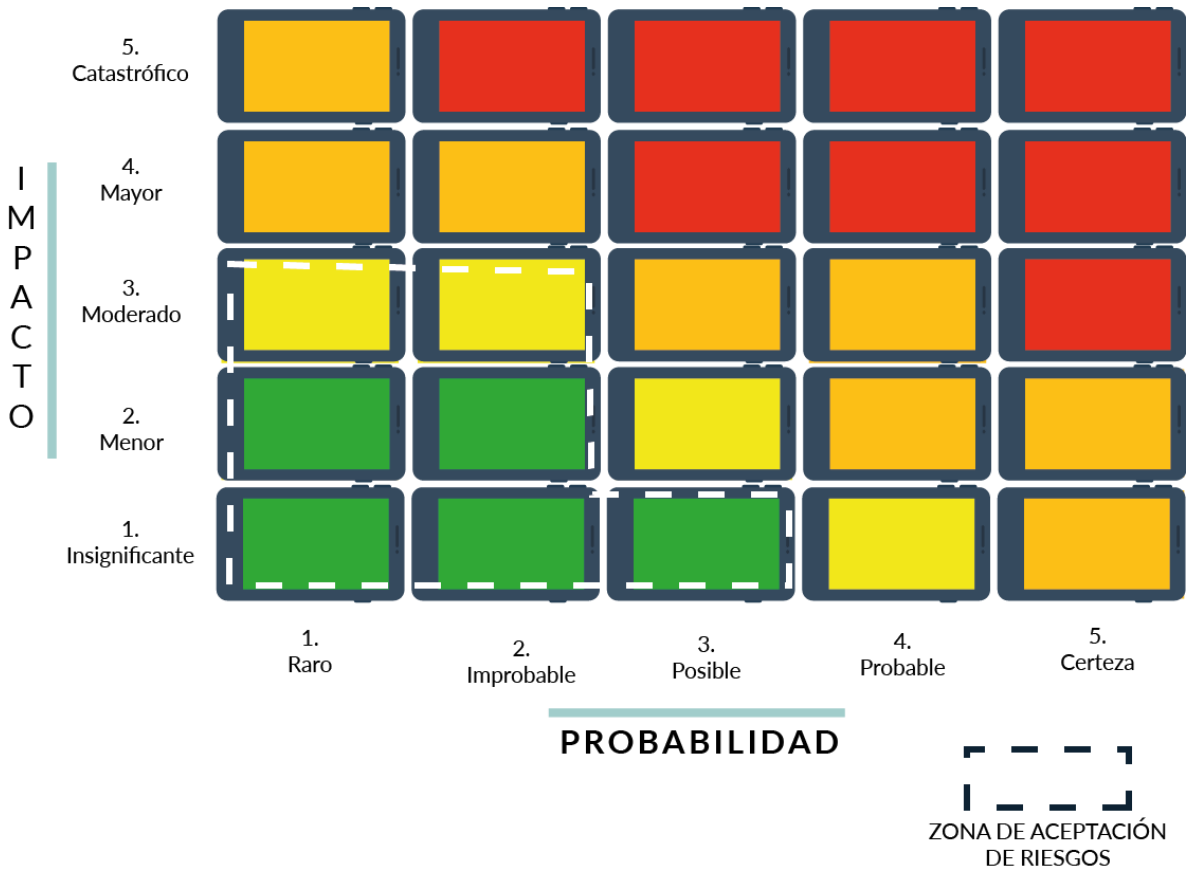

Imagen 3. Mapa de calor con definición del apetito de riesgo. Fuente: elaborado por el autor

4.2 Fase 2. Ejecución de la GRSD

Una vez ejecutada la fase anterior Planificación de la GRSD, la entidad procede a realizar las siguientes actividades, en orden secuencial:

4.2.1 Identificación de activos de información

Para la identificación de activos de información, la entidad debe:

- ✓ Realizar un inventario de los activos de información por cada proceso
- ✓ Identificar el dueño del riesgo sobre el activo y el responsable del activo de información
- ✓ Clasificar los activos
- ✓ Determinar el nivel de importancia del activo

- ✓ Identificar si existe Infraestructura crítica cibernética (ICC)
- ✓ Identificar activos de TI/TO asociados a la Infraestructura crítica cibernética (ICC)
- ✓ Clasificar la información

Realizar un inventario de los activos de información por cada proceso: los activos de información deben ser identificados por medio de:

- ✓ Un consecutivo: corresponde al número consecutivo de los activos. Ej. A1, A2, etc.
- ✓ Un nombre: corresponde al nombre que se le va a dar al activo. Ej. Firewall.

Identificar el dueño del riesgo sobre el activo y el responsable del activo de información: la entidad debe identificar el dueño del riesgo sobre el activo y responsable o dueño del activo de información:

- ✓ Dueño del riesgo o custodio sobre el activo: persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. Ej. Técnico en operaciones.
- ✓ Responsable o dueño del activo de información: cargo de la persona responsable del activo. Ej. jefe de operaciones.

Clasificar el activo: determinar la clasificación de acuerdo con el tipo de activo de información; a continuación, se relacionan algunos tipos de activos, sin limitarse, a los que pueda definir la entidad:

Tabla 4. Ejemplo de clasificación de activos

Clasificación del activo	Descripción
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
Documentos información	Datos e información almacenada o procesada física o lógicamente, tales como: 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, entre otros
Software	Activo informático lógico como aplicaciones, programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como *routers*, servidores, *switches*, biométricos que por su criticidad son considerados activos de información
Servicios	Prestación de un servicio por parte de una compañía para el apoyo de las actividades de los procesos, tales como: internet, páginas de consulta, etc.
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa y el *good will*, entre otros
Datos/bases de datos	Conjunto de datos y registros lógicos ingresados en las aplicaciones o servidores que a su vez quedan almacenados en un repositorio de datos centralizado. Puede considerarse base de datos, la información alojada en las aplicaciones de contabilidad y nomina, entre otras
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, entre otros
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: elaborado por el autor

Determinar el nivel de importancia del activo: para determinarlo se sugieren las siguientes premisas; sin embargo, la entidad puede formular preguntas adicionales que le permitan cumplir con este objetivo:

Tabla 5. Ejemplo de preguntas para determinar el nivel de importancia de los activos

Nivel de importancia del activo		
Pregunta	**Opciones de respuesta**	
	Sí	**No**
¿El activo pertenece a la entidad o a terceros?	El activo de información es propio de la entidad.	El activo de información es de propiedad de un tercero y es custodiado de forma temporal o permanente por la entidad
¿Debe ser restringido a un número limitado de usuarios?	El activo de información es manejado solamente por un área específica de la entidad	El activo de información es de conocimiento público o de uso de todos los funcionarios de la entidad
¿Es muy crítico para las operaciones internas?	El activo de información es crítico para la operación, ya que compromete la confidencialidad, integridad o disponibilidad de la información de la entidad	El activo de información no es crítico para la operación ya que no compromete la confidencialidad, integridad o disponibilidad de la información de la entidad
¿Es muy crítico para el servicio hacia terceros?	La gestión del activo de información afecta de manera directa o importante el servicio que se presta hacia terceros	La gestión del activo de información afecta de manera indirecta o poco representativa el servicio que se presta hacia terceros
En caso de ser conocido, utilizado o modificado por alguna persona o sistema, sin la debida autorización, impactarían negativamente a los sistemas y procesos de la empresa, de manera:		
Impacto	**Criterio de evaluación**	
Leve	La modificación no autorizada del activo de información afecta de forma moderada la seguridad de la información	
Importante	La modificación no autorizada del activo de información afecta de manera representativa la seguridad de la información	
Grave	La modificación no autorizada del activo de información afecta de manera seria la seguridad de la información	

Fuente: elaborado por el autor

Nota: para determinar el nivel de importancia del activo, la entidad puede definir unos valores para cada criterio (opción de respuesta), realizar un promedio entre dichos valores y determinar el nivel de importancia el cual puede ser alto, medio o bajo.

Identificar si existe Infraestructura crítica cibernética: culminado el paso anterior, la entidad debe determinar si los procesos en los cuales identificó los activos de información, son servicios esenciales y si estos hacen parte de la

infraestructura crítica cibernética (ICC) del país. Para la ejecución de esta actividad se debe tomar como base la guía para la identificación de infraestructura crítica cibernética de Colombia, primera edición, emitida por el comando conjunto cibernético (CCOC). Si la entidad cuenta con ICC debe reportarla al CCOC.

Nota: la entidad debe determinar si los activos identificados proveen servicios esenciales, entendidos estos como "los necesarios para el mantenimiento de las funciones sociales básicas, salud, seguridad, bienestar social y económico de los ciudadanos o el funcionamiento de las instituciones del Estado y de las administraciones públicas".[8]

4.2.1.1 Identificar activos de TI/TO asociados a la ICC

Una vez la entidad ha determinado que cuenta con ICC, debe identificar cuáles son los activos de tecnologías de información (TI) y activos de tecnologías de operación (TO) asociados a esta infraestructura. Para la ejecución de esta actividad, la entidad debe tomar como referencia la guía de ICC de acuerdo con el sector correspondiente, la cual define una serie de activos de tecnologías de información (TI) y tecnologías de operación (TO).

Nota: la guía de ICC del sector que toma como referencia, está determinada por la misión de cada entidad.

Clasificar la información: la entidad debe clasificar los activos de información identificados e incluir los activos de infraestructura crítica cibernética, de acuerdo con la ley de transparencia y del derecho de acceso a la información pública nacional, ley 1712:2014, principalmente los relacionados en el artículo 6.

Tabla 6. Clasificación de la información

[8]Tomado de la guía para la identificación de infraestructura crítica cibernética de Colombia, primera edición. Emitida por el comando conjunto cibernético (CCOC).

Tipos de clasificación	Descripción
Información pública	Es toda información que un sujeto obligado genere, obtenga, adquiera o controle
Información pública clasificada	Es aquella información que al estar en poder o custodia de un sujeto obligado, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica, por lo que su acceso puede ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en al artículo 18 de esta ley.
Información pública reservada	Es aquella información que al estar en poder o custodia de un sujeto obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Fuente: ley 1712/2014

Nota: adicional a lo anterior, la guía 5 para la gestión y clasificación de activos, estrategia Gobierno en línea (GEL) MinTIC, capítulo 7, también es una orientación para clasificar los activos de información en el marco del MSPI.

4.2.2 Identificar los riesgos inherentes de seguridad digital

Los riesgos se deben identificar basados en las amenazas y vulnerabilidades asociadas al activo de información sobre el cual se está haciendo la identificación. En este caso, hay referencias que permiten vislumbrar la claridad que hay que tener para esta definición, en este caso los anexos de la NTC ISO27005:2011.

Identificación de amenazas: las amenazas representan situaciones o fuentes que pueden hacer daño a los activos digitales. A manera de ejemplo se citan las siguientes amenazas:

- ✓ Deliberadas (D), fortuito (F) o ambientales (A).

Tabla 7. Tabla de amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: MinTIC

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

Tabla 8. Tabla de amenazas dirigida por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Fuente: MinTIC

Nota: si la entidad cuenta con ICC para identificar las amenazas asociadas a los activos de tecnologías de información (TI) y tecnologías de operación (TO) de estas infraestructuras, tome como referencia la guía de ICC del sector de su interés.

Identificación de vulnerabilidades: la entidad puede identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización de la entidad
- ✓ Procesos y procedimientos
- ✓ Rutinas de gestión
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información
- ✓ *Hardware, software* y equipos de comunicaciones
- ✓ Dependencia de partes externas
- ✓ Otras áreas donde se transmita o almacene información digital

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 relacionan ejemplos de vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tabla 9.Ejemplos de vulnerabilidades y amenazas

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Ubicación física de los equipos Fallas en la configuración del *hardware* Valor económico de los equipos	Incumplimiento en el mantenimiento del sistema de información
Software	Ausencia o insuficiencia de pruebas de software Obsolescencia de *software*	Abuso de los derechos
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
Bases de datos	Obsolescencia de base de datos Valor económico de datos	Obsolescencia
Personal	Error humano Ausencia de soporte por parte del fabricante Mantenimiento no adecuado de los equipos	Incumplimiento en la disponibilidad del personal
Tipo organización	Falta de planeación Administración de seguridad insuficiente	Abuso de los derechos

Fuente: elaborado por el autor

Nota: si la entidad cuenta con infraestructura crítica cibernética (ICC) para identificar las vulnerabilidades asociadas a los activos de tecnologías de información (TI) y tecnologías de operación (TO) de estas infraestructuras, tome como referencia la guía de ICC del sector de su interés.

Identificación del riesgo inherente de seguridad digital: para cada tipo de activo hay una serie de riesgos, los cuales la entidad debe identificar. A continuación, se relacionan ejemplos de riesgos con sus respectivas amenazas y vulnerabilidades de acuerdo con el tipo de activos.

Tabla 10. Ejemplos de riesgos asociados a las amenazas y vulnerabilidades

Tipo de activo	Amenazas	Vulnerabilidades	Riesgo
Software	Exceso de confianza	Ausencia de un procedimiento escrito para el desarrollo y cambios de *software*	Modificación no autorizada de información o configuración
Base de datos	*Hackeo* no ético	Contraseñas de bases de datos no seguras	Modificación sin autorización
Red	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes	Fraude y robo de información
Software	Personal externo	Administración inadecuada de la base de datos	Daño o mal funcionamiento
Hardware	Ubicación física de los equipos	Incumplimiento en el mantenimiento del sistema de información	Fallas en la prestación de servicios

Fuente: elaborado por el autor

La identificación de riesgos también 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, casos ocurridos que los participantes conozcan que se hayan dado en la entidad 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 digital 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, listas de chequeo.

Nota: si la entidad cuenta con ICC para identificar los riesgos asociados a las amenazas y vulnerabilidades de tecnologías de información (TI) y tecnologías de operación (TO), tome como referencia la guía de ICC del sector de su interés.

4.2.3 Valoración de riesgos inherentes de seguridad digital

Para llevar a cabo la valoración del riesgo inherente de todos los activos incluidos los de ICC, deben identificarse previamente los siguientes aspectos:

- ✓ Probabilidad de ocurrencia
- ✓ Impacto asociado a las variables confidencialidad, integridad, disponibilidad, social, económica y ambiental

Nota: al evaluar el impacto de los riesgos asociados a cada activo, es importante aclarar que no necesariamente todos los criterios deben ser evaluados, ya que dependen de la naturaleza de la entidad, el tipo de activo y de la pertinencia que tenga cada variable en la medición del impacto.

4.2.3.1 Determinación probabilidad de ocurrencia e impacto

Una vez definidos los riesgos, las amenazas y las vulnerabilidades se calcula la probabilidad de ocurrencia y el impacto para cada uno de los riesgos y se toma como base los criterios definidos en la fase de planificación.

Para el caso del impacto, es claro que se definieron cinco niveles asignados (insignificante, menor, moderado, mayor y catastrófico) para seis variables a saber:

confidencialidad, integridad, disponibilidad, social, económico y ambiental. Es importante estimar que la calificación del impacto que pueda generar o establecer el riesgo analizado, como fue mencionado anteriormente en el del numeral 4.2.3, no necesariamente aplica a todas las seis variables. Por lo tanto, se deben considerar solamente aquellas que realmente sirvan para el análisis. El impacto total puede ser la combinación de los valores aplicados en un promedio. El resultado del riesgo inherente está determinado por la relación entre la probabilidad y el impacto.

De esta manera, se busca establecer cuál es el nivel de riesgo sin considerar la existencia de ningún control, así se logra obtener el nivel de riesgo inherente. Por ejemplo:

Se identifica un riesgo de acceso no autorizado a una base de datos, la cual es un activo muy importante para una entidad del Gobierno colombiano.

> **Probabilidad:** según registros, esta situación es *posible*. Por lo tanto, de acuerdo con los criterios de probabilidad definidos tiene una valoración de tres.
>
> **Impacto:** según el análisis de la información realizada por el experto de la entidad, se determinan los siguientes valores:
>
> - Impacto social (1- insignificante)
> - Económico (3 - moderado)
> - Confidencialidad (2 - menor)
> - Integridad (2 - menor)

Nota: en el presente ejemplo se calcularon cuatro variables únicamente. De acuerdo con lo anterior, la entidad puede calcular las variables para las cuales tienen información o son relevantes, dentro del proceso o activo evaluado.

Análisis: el experto que analiza esta situación, al obtener el promedio de estas cuatro variables afectadas por este riesgo, determina que el Impacto de este riesgo es 2 (menor).

Tabla 11. Ejemplo valoración del riesgo inherente de seguridad digital

Ejemplo: valoración del riesgo inherente de seguridad digital									
Riesgo	Probabilidad de ocurrencia	**Impacto** Social	Económico	Ambiental	Confidencialidad	Integridad	Disponibilidad	Impacto del riesgo	Zona de riesgo
Acceso no autorizado a una base de datos	3-posible	1-insignificante	3-moderado		2- menor	2- menor		2- menor	Zona de riesgo medio

Fuente: elaborado por el autor

- ✓ **Zona de Riesgo:** el riesgo se ubica en la zona 6 (medio), dado que la probabilidad es tres3 y el impacto es dos. A continuación se presenta el ejemplo de ubicación del riesgo.

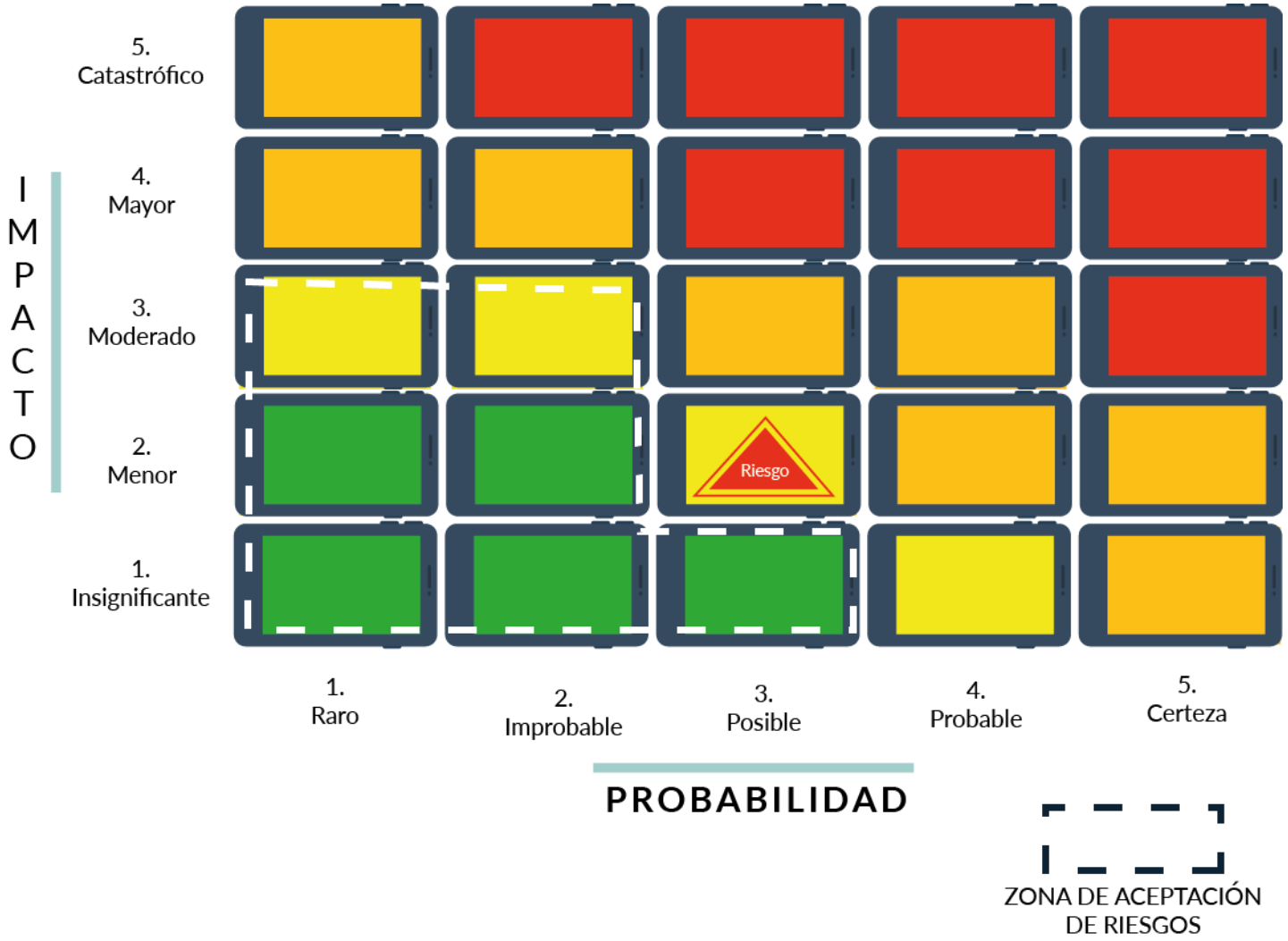

Imagen 4. Ejemplo determinación probabilidad de ocurrencia e impacto. Fuente: elaborado por el autor

4.2.4 Identificación y evaluación de los controles

Una vez establecidos los riesgos inherentes se procede a la identificación y evaluación de los controles; para esto se puede tomar como referencia lo definido en la guía para la administración del riesgo de la función pública[9] o lo establecido a continuación:

Notas:

- Determinar si existe uno o varios controles asociados a los riesgos inherentes identificados.
- Si no hay controles asociados a los riesgos inherentes identificados, entonces se registra y se aplica un tratamiento inmediato que implique la implementación de alguna actividad compensatoria, en este caso el nivel de riesgo seguiría igual ya que no se evidenciaría ningún desplazamiento en el mapa de calor.
- Si los controles existen, se realiza la identificación de los criterios para la evaluación de acuerdo con las características de los controles.

Cualidades de los controles

Tabla 12. Cualidades de los controles

Cualidades	
¿El control existe?	Evidencia de la existencia o no de un control para la gestión del riesgo de la actividad evaluada
¿Se considera un control clave[10]?	Esta variable se tiene en cuenta cuando el control identificado se considera de manera vital y es necesaria la ejecución para la gestión del riesgo evaluado

[9]Para la evaluación de controles puede tener en cuenta lo definido en la guía para la administración del riesgo de la función pública págs. 24, 25, 26 y 27, https://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADa+de+Riesgos+y+Caja+de+Herramientas.rar/a125ddf9-8a7b-4615-860c-2c63c38ad74a.

[10] Se puede considerar un control clave aquel que opera con la misión de cumplir, a través de sus actividades, con la mitigación clara de riesgos y que sin este control se expone a la pérdida de

Fuente: elaborado por el autor

Características de controles. A continuación, se presentan algunas características de los controles a manera de ejemplo, para lo cual se toma como referencia lo definido en la guía para la administración del riesgo de la función pública[11]. La entidad puede adoptarlas, desarrollarlas o referenciarse de acuerdo con sus criterios.

Tabla 13. Características de los controles

Características	
Categoría o niveles del control	Se dan los siguientes tipos de control de acuerdo con los niveles que desarrollan las entidades. **Operativo:** considera cada tarea u operación. Orientado a corto plazo. **Táctico:** considera cada unidad de la empresa (departamento) o cada conjunto de recursos por separado. Orientado a mediano plazo. **Estratégico:** considera a la empresa en su totalidad como un sistema. Orientado a largo plazo.
Naturaleza del control	La naturaleza del control se refiere a las siguientes posibilidades: **Manual:** control donde existe la presencia y la intervención de una persona; ejemplo: autorizaciones a través de firmas. **Mixto:** control donde existe la presencia y la intervención de una persona y una máquina; ejemplo: control de video cámaras. **Automático:** utilizan herramientas tecnológicas; ejemplo: sistemas de información.
Documentación	Esta característica se refiere a determinar si: ¿El control está documentado? ¿El control no está documentado?
Complejidad	Esta característica establece el grado de complejidad de la ejecución del control: ¿El control es complejo para ejecutar? ¿El control no es complejo para ejecutar?
Tipo de control	**Preventivo:** evitan que un evento suceda. Actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos; ejemplo una clave de acceso. **Detectivos:** se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o automáticos. Sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear o alertar a los funcionarios; ejemplo: un cortafuegos o *firewall*.

integridad de la información o del normal funcionamiento de la operación del negocio o de la misión de la entidad.

	Correctivo: estos no prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Permiten el restablecimiento de una actividad, después de ser detectado un evento no deseable y posibilita la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan y permiten mejorar las deficiencias. Por lo general, actúan con los controles detectivos, implicando reprocesos. Son de tipo administrativo y requieren políticas o procedimientos para su ejecución; ejemplo: la restauración de una copia de seguridad o *back up*.
Importancia sobre la mitigación del riesgo	Percepción del dueño del riesgo, del riesgo del activo: establece si este control es relevante para mitigar el riesgo: importante o no importante.
Responsable del control	Significa establecer si: ¿El control tiene asignado un responsable? ¿El control no tiene asignado o definido un responsable?
Puede disminuir la probabilidad	Percepción del dueño del riesgo: establece si el control llega a disminuir la probabilidad de ocurrencia del riesgo: si/no.
Puede disminuir el impacto	Percepción del dueño del riesgo: establece si el control llega a disminuir el impacto del riesgo: si/no.

Fuente: elaborado por el autor

Una vez que la entidad identifique los controles, debe realizar un análisis y tener en cuenta las características; esto con el fin de determinar el grado de efectividad que se ve reflejado con desplazamiento del riesgo dentro del mapa de calor. Por ejemplo:

Para mayor entendimiento de esta actividad y continuando con el ejemplo anterior, se ponderan las características de tres controles asociados al riesgo de “acceso no autorizado a una base de datos”. Si la entidad aún no ha valorado los controles, puede seguir este ejemplo o tomar como referencia lo definido en la guía para la administración del riesgo de la función pública (DAFP). Los controles se evalúan acorde con sus posibles valores.

Tabla 14. Análisis y evaluación de controles

Descripción del control	Criterios de evaluación	Consideración de variables	Evaluación de control 1	Evaluación de control 2	Evaluación de control 3
Control 1. La segregación de funciones para el administrador de la base de datos.	Categoría del control	Manual = 1 Mixto = 2 Automático = 3	3	2	3
	Naturaleza del control	Estratégico = 1 Táctico = 2 Operativo = 3	3	2	3
Control 2. El uso de una herramienta automática que registra las transacciones que este administrador realiza.	Documentación	Sí existe = 1 No existe = 0	1	0	0
	Complejidad	Complejo para ejecutar = 1 No complejo = 0	1	0	0
	Responsable del control	Asignado = 1 No asignado = 0	1	0	0
	Tipo de control	Preventivo = 3 Detectivo = 2 Correctivo = 1	3	1	3
	Importancia sobre la mitigación del riesgo	Si = 1 No = 0	1	0	0
Control 3. Monitoreo de actividades del DBA.	Puede disminuir la Probabilidad	Si = 1 No = 0	1	0	1
	Puede disminuir el impacto	Si = 1 No = 0	1	0	0
		Total	15	5	10

Fuente: elaborado por el autor

Tabla 15. Rango de calificación de los controles

Rango para determinar el nivel de efectividad de los controles	Criterios de desplazamiento de impacto o probabilidad en la evaluación del riesgo
Control(es) no efectivo(s) entre 0 y menor o igual a 5	Se mantiene en el mismo nivel de impacto y probabilidad.
Control(es) efectivo(s) mayor a 5 y menor o igual a 10	Se desplaza la probabilidad a la izquierda un cuadrante, si la característica de “puede disminuir la probabilidad” es igual a uno o cuando hay más de un control, el promedio de la calificación de esta misma característica sea igual o superior a 0,5 y, Se desplaza el impacto hacia abajo un cuadrante si la variable de la característica de “puede disminuir el impacto” es igual a uno o cuando hay más de un control, el promedio de la

	calificación de esta misma característica sea igual o superior a 0,5.
Control(es) muy efectivo(s) mayor a 10 y menor o igual a 15	Se desplaza la probabilidad a la izquierda dos cuadrantes si la característica de “puede disminuir la probabilidad” es igual a uno o cuando hay más de un control, el promedio de la calificación de esta misma característica sea igual o superior a 0,5 y, Se desplaza el impacto hacia abajo dos cuadrantes si la variable de la característica de “puede disminuir el impacto” es igual a uno o cuando hay más de un control, el promedio de la calificación de esta misma característica sea igual o superior a 0,5.

Fuente: elaborado por el autor.

El promedio de los tres controles evaluados es de diez, valor que debe ser comparado con los rangos de la tabla que a continuación determina el nivel de efectividad. En este caso es un control efectivo que dadas las circunstancias desplazaría un cuadrante.

En el ejemplo de los tres controles que se acaban de evaluar, el control resultó efectivo, pero solamente se desplazó en probabilidad y no en impacto, dado que el promedio de las características mencionadas en el criterio de desplazamiento, establece que el promedio de “puede disminuir la probabilidad” es 0,66 y el promedio de “puede disminuir el impacto” es de 0,33, lo cual, según los criterios, solo desplaza hacia la izquierda un cuadrante.

Nota: si la entidad cuenta con ICC para identificar los controles asociados a estas infraestructuras de tecnologías de información (TI) y tecnologías de operación (TO), tome como referencia la guía de ICC del sector de su interés.

Determinación del riesgo residual: una vez evaluados los controles, se calculó de acuerdo con el ejemplo la probabilidad y el impacto para determinar el riesgo residual. La calificación del control determina si se disminuyen o no los niveles de

probabilidad e impacto. De ser así, el riesgo inherente se desplaza en el mapa de calor y se obtiene el riesgo residual. Por ejemplo:

Continuando con el ejemplo anterior relacionado con “riesgo de acceso no autorizado a una base de datos”, el riesgo inherente está ubicado en zona de riesgo medio (probabilidad 3, impacto 2). Este riesgo cuenta con tres controles asociados: 1. la segregación de funciones para el administrador de la base de datos, 2. el uso de una herramienta automática que registra las transacciones que este administrador realiza y 3. monitoreo de actividades del DBA.

Características: luego de evaluar las características del control se determina qué es efectivo y qué desplaza únicamente la probabilidad a un valor menor (menos probable); es decir, deja la probabilidad en 2 (improbable). El valor del impacto continúa en 2.

Riesgo residual: con la probabilidad desplazada a 2 y el impacto que se mantiene en 2, el riesgo residual es 4 (bajo); es decir, probabilidad (improbable = 2) e impacto (menor = 2).

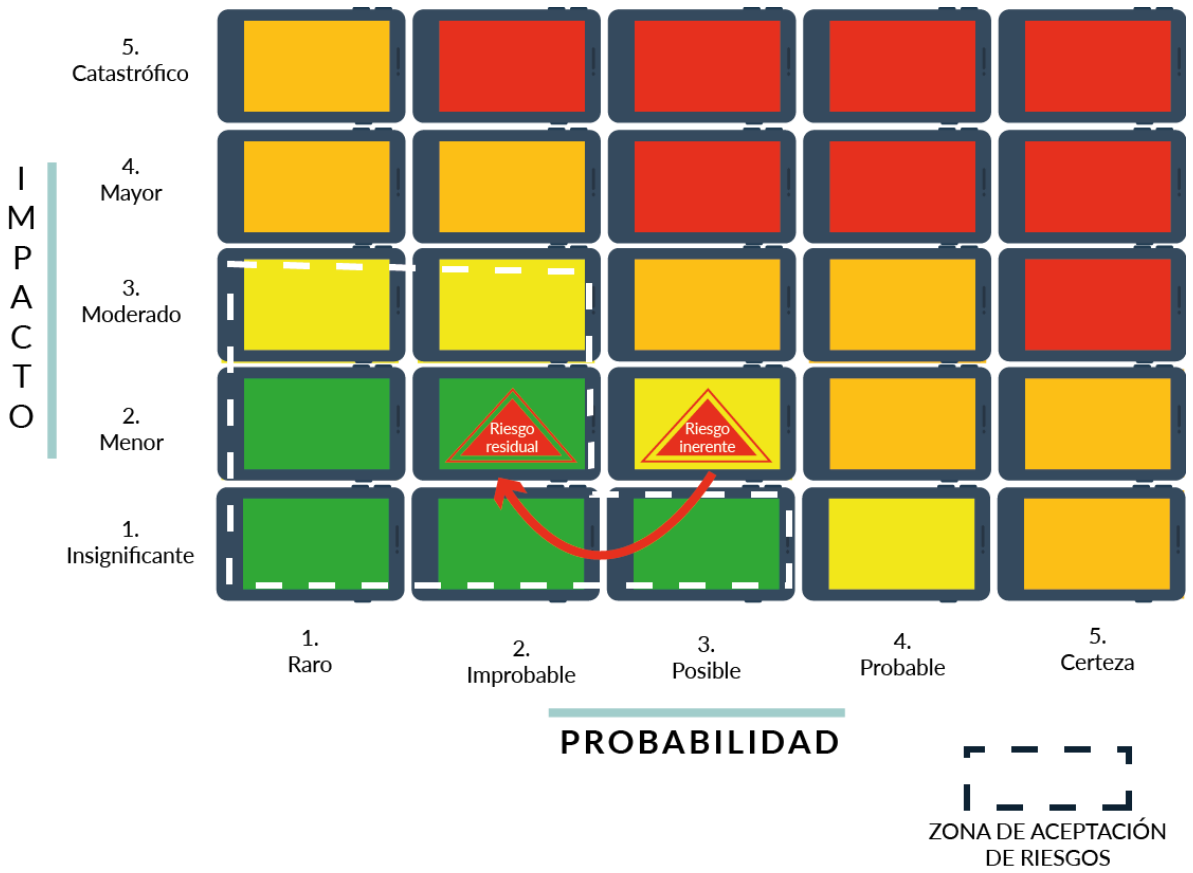

Imagen 5. Determinación del riesgo residual. Fuente: elaborado por el autor

Nota: en el ejemplo propuesto, se evidencia que el impacto al disminuir se desplaza "verticalmente hacia abajo" y la probabilidad disminuye "horizontalmente hacia la izquierda".

4.2.5 Tratamiento de los riesgos de seguridad digital

Una vez se han identificado los riesgos residuales, la entidad debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos en la etapa de planificación.

4.2.5.1 Identifique opciones de tratamiento para los riesgos de seguridad digital

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad puede tener en cuenta las siguientes opciones:

Evitar el riesgo: la entidad decide no iniciar o continuar con la actividad que lo originó.

Aceptar el riesgo: tomar o incrementar el riesgo para perseguir una oportunidad. Igualmente, aquellos riesgos a nivel residual, que se encuentren en zona de apetito de riesgo, deben ser adoptados de igual forma, aunque monitoreados para evitar que se aumenten los niveles ya sea de probabilidad o de impacto.

Transferir el riesgo: si la entidad no puede o no desea asumir la gestión del riesgo, entonces puede transferirlo a terceros o compartirlo con otra entidad.

Establecer nuevos controles: implementar nuevos controles de seguridad que sean efectivos y eficaces para disminuir la probabilidad y el impacto del riesgo.

Nota: si la entidad cuenta con ICC, para identificar los controles asociados a estas infraestructuras, de tecnologías de información (TI) y tecnologías de operación (TO), tome como referencia la guía de ICC del sector de su interés. Por ejemplo:

Continuando con el ejemplo anterior, relacionado con “riesgo de acceso no autorizado a una base de datos”, se puede suponer una situación en donde la entidad no puede costear una aplicación para registrar las actividades del administrador de base de datos (control dos propuesto). Por lo tanto, la entidad decide “transferir” el riesgo subcontratando un servicio de monitoreo o administración delegada, a bajo costo, con una empresa especializada en este tipo de servicios.

Priorizar los tratamientos: la entidad debe definir las acciones que debe seguir para priorizar los tratamientos de acuerdo con el impacto del riesgo residual. Tome como referencia el siguiente ejemplo:

Tabla 16. Ejemplos de planes de acción para el tratamiento de riesgos

Acción	Descripción
Acción inmediata	Considerar el plan de tratamiento a muy corto plazo, es decir, el nivel de riesgo de seguridad digital puede afectar considerablemente factores sociales, económicos, ambientales; además de la confidencialidad, integridad y disponibilidad de la información.
Decisión importante	Considerar el plan de tratamiento a corto plazo, es decir, el nivel de riesgo de seguridad digital puede afectar factores sociales, económicos, ambientales; además de la confidencialidad, integridad y disponibilidad de la información.
Decisión normal	Considerar el plan de tratamiento a mediano plazo, es decir, el nivel de riesgo de seguridad digital no puede afectar de forma inmediata factores sociales, económicos, ambientales; además de la confidencialidad, integridad y disponibilidad de la información, pero se requiere gestionar el riesgo, ejecutando controles o fortaleciendo los ya existentes, de tal forma que no se desplacen a niveles superiores.
Mantener nivel	Considerar a mediano o largo plazo en el plan de tratamiento la posibilidad de convivir con el nivel de riesgo de seguridad digital monitoreando la efectividad de los controles o en su defecto, pensar en alternativas de mitigación e implementar controles complementarios o transferir a un tercero el riesgo de seguridad de la información.
Evaluar aceptación	Considerar permanentemente el nivel de monitoreo de la efectividad de los controles sobre los riesgos de seguridad digital y mantener intactos en el tiempo los niveles de impacto y probabilidad.

Fuente: elaborado por el autor

El plan de tratamiento se convierte en una herramienta de ruta crítica sobre la cual se definen responsables, recursos y tiempos para lograr el propósito definido como parte de la gestión de riesgo de seguridad digital.

Nota: la ejecución del plan de tratamiento de los riesgos de seguridad digital es responsabilidad de cada entidad y solamente ella es la que define y puede disponer de los recursos necesarios para la definición de dicho plan.

Seguimiento al plan de tratamiento: la entidad debe hacer un seguimiento al plan 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.
- ✓ Documentar los resultados de los planes de acción que ponga en marcha.
- ✓ Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.

Nota: una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad 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.

4.3 Fase 3. Monitoreo y revisión

En esta fase se debe evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles, de acuerdo con lo definido por la entidad, así mismo, contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la alta dirección y las partes interesadas internas.

4.3.1 Registro y reporte de eventos de riesgos de seguridad digital

Es importante que la entidad cuente con registro de los incidentes de riesgos de seguridad digital que se han materializado, con el fin de analizar las causas, las deficiencias de los controles y las pérdidas que se pueden generar.

4.3.1.1 Reporte de la gestión del riesgo de seguridad digital al interior de la entidad

La entidad debe reportar periódicamente a la alta dirección y a las partes interesadas la siguiente información:

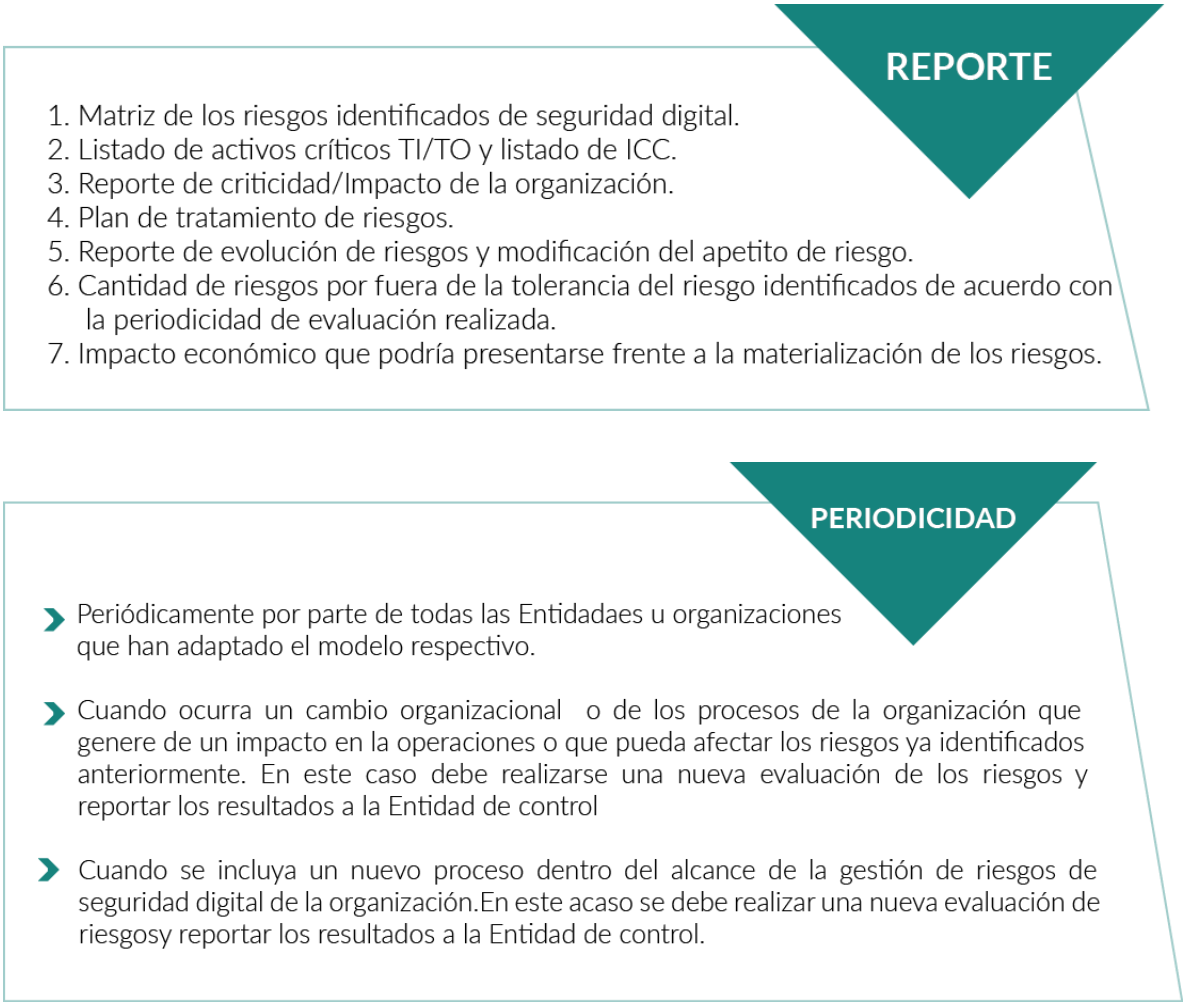

Imagen 6. Reporte de información por parte de la entidad. Fuente: MinTIC

4.3.1.2 Reporte de la gestión del riesgo de seguridad digital a grupos de interés especial

Una vez la Entidad obtenga los resultados de la gestión de riesgos de seguridad digital (GRSD) deberá consolidar la siguiente información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a los grupos de interés especial según se indicará a continuación:

Información a consolidar:

- Activos digitales críticos

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Servicios digitales críticos
- Las infraestructuras críticas cibernéticas (ICC) identificadas y los riesgos, amenazas y vulnerabilidades relacionados con estas.

Reporte a entidades de interés especial:

Los activos y servicios digitales críticos (aquellos que afectan gravemente al funcionamiento de la entidad) y los riesgos, amenazas y vulnerabilidades más importantes identificados durante el ejercicio de riesgos, deberán ser reportados al CSIRT de Gobierno.

Reporte si se es operador o dueño de Infraestructuras Críticas Cibernéticas:

Sean entidades públicas o privadas, las infraestructuras críticas cibernéticas (ICC) que hayan sido identificadas y los riesgos, amenazas y vulnerabilidades críticas relacionados con estas, deberán reportarse al CCOC, dado que es la entidad encargada de administrar esta información.

Nota 1: Estos reportes son de obligatorio cumplimiento para las entidades públicas.

Nota 2: Los reportes previos se realizarán empleando los controles necesarios para garantizar la seguridad y confidencialidad de la información contenidos en ellos (Acuerdos de confidencialidad y controles técnicos adecuados).

Es importante indicar que los reportes de riesgos de seguridad digital a las entidades de interés especial indicados previamente, no implican o significan el traslado de la responsabilidad sobre los riesgos o su tratamiento.

4.3.2 Auditorías internas y externas

Deben programarse y ejecutar auditorías [12] internas y externas con fechas planificadas, las cuales deben quedar registradas en el plan anual de auditoría.

4.3.3 Revisión por parte de la alta dirección

La alta dirección de la entidad debe realizar revisiones periódicas y el respectivo seguimiento al proceso de gestión de riesgo de seguridad digital.

4.3.4 Medición del desempeño

La entidad debe utilizar medidas de desempeño[13] para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente.

4.3.5 Rendición de cuentas

Las múltiples partes interesadas deben rendir cuentas sobre la base de las funciones, capacidad para actuar y tener en cuenta el posible impacto de las decisiones. También deben reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.[14]

---

[12] Para realizar el monitoreo y revisión mediante auditoría, tome en cuenta lo definido en la guía número 15 del modelo de seguridad de la información *Guía de auditoría* del MinTIC, estrategia Gobierno en línea (GEL).6

[13]Para realizar la medición del desempeño, tome en cuenta lo definido en la guía número 16 del modelo de seguridad de la información *Guía de evaluación del desempeño* del MinTIC, estrategia Gobierno en línea (GEL).

[14]CONPES 3854.

4.4 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad digital

La entidad debe propender por la mejora continua[15] de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que:

Cuando existan hallazgos, la entidad debe mitigar el impacto de su existencia y tomar acciones para controlarla y prevenirla. Adicionalmente, establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para disminuir las causas de las no conformidades de la siguiente forma:

- ✓ Revisar y evaluar la no conformidad encontrada
- ✓ Establecer las posibles causas y consecuencias que se generaron con la no conformidad
- ✓ Determinar si existen otras no conformidades similares para establecer acciones correctivas y evitar así que se lleguen a materializar
- ✓ Emprender acciones detectivas que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de otras no conformidades

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado a la no conformidad, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuras no conformidades.

[15]Para esta fase de mejoramiento continuo, tome en cuenta lo definido en la guía número 17 del modelo de seguridad de la información *Guía de mejora continua* de MinTIC, estrategia Gobierno en línea (GEL).

4.4.1 Comunicación y consulta

Esta fase es transversal a toda la gestión de riesgo de seguridad digital. Por lo tanto, se considera una fase esencial dado que permite asegurar su entendimiento por parte de las múltiples partes interesadas.

4.4.1.1 ¿Cómo realizar la comunicación y consulta?

Para la ejecución de esta fase, la entidad debe establecer o asegurarse de contar con un plan de comunicación, el cual especifique como mínimo los siguientes aspectos:

- Qué se va a comunicar
- Cómo se va a comunicar
- Medios de comunicación
- Quién lo comunica
- Cuándo se comunica
- A quién se comunica (grupos de partes interesadas)

A continuación, se presenta una matriz de comunicación a manera de ejemplo:

Tabla 17. Ejemplo de una matriz de comunicación

Qué comunica	Cómo comunicar	Vía de comunicación	Quién lo comunica	Cuándo se comunica	A quién se comunica
Compromiso por la alta dirección, políticas y objetivos del sistema de Gestión de Riesgos	Inducción Reinducción Capacitaciones Avisos	Escrita	Jefes inmediatos Área de Recursos Humanos	Permanente según lo definido en el plan de comunicación	Partes interesadas internas

Fuente: elaborado por el autor