GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN EL **SECTOR PRIVADO Y MIXTO**

GOBIERNO DE COLOMBIA

Tabla De Contenido

Índice de tablas

Tabla de imágenes

ANEXOS

ANEXO 1. Ejemplo aplicación de la guía.

Introducción

La gestión de riesgo de seguridad digital se ha convertido en un reto para el Gobierno de Colombia, el cual es consciente de la importancia tan relevante que los sistemas, redes de información y la interacción entre ellos son vitales para asegurar la estabilidad y eficiencia de la economía y el comercio a nivel nacional e internacional, así como de la vida social, cultural y política.

El Gobierno Nacional, consciente de la expansión que han desarrollado en los últimos años los sistemas y redes de información los cuales vienen con nuevos retos y riesgos, se ha empeñado por ser pionero en la seguridad digital. Es así que actualmente es pionero en Latinoamérica en estudiar el impacto de las amenazas digitales en diferentes sectores productivos y en determinar que la seguridad digital es responsabilidad de todos y que cada actor de las múltiples partes interesadas. Por lo anterior el Gobierno Nacional debe velar por dicha seguridad, proteger su información en el mundo digital y redoblar los esfuerzos a través de políticas e iniciativas, para tomar medidas preventivas ante los posibles ataques en el entorno digital.

MINTIC, pretende fortalecer el entorno digital a través de un modelo de gestión de riesgos de seguridad digital (MGRSD), el cual complementará el componente de seguridad y privacidad de la información. Este Modelo, tiene como objetivo establecer la Gestión de Riesgos de Seguridad Digital (GRSD) en las organizaciones que decidan aplicarlo y con mayor razón cuando tengan infraestructuras criticas cibernéticas asociadas. Por tanto, como parte especifica del MGRSD, se definieron las Guías de orientación para la gestión de riesgos de seguridad digital de los sectores Gobierno Nacional, territoriales y sector público, mixto y privado, así como fuerza pública, las cuales consignan la información de cómo las organizaciones deben adoptar la GRSD

Por otra parte, se definió la presente guía, la cual tiene como objetivo orientar a las organizaciones del sector privado y mixto en el desarrollo de la metodología para la gestión de riesgos de seguridad digital (GRSD), enmarcadas en un ciclo Deming PHVA[1], para un mayor entendimiento e integración con los sistemas de gestión implementados en las diferentes organizaciones.

De igual manera orientar a las organizaciones del sector privado y mixto que han identificado infraestructuras criticas cibernéticas (ICC) de orden nacional en la forma como debe gestionar los riesgos asociados a estas ICC y a los asociados a las Tecnologías de Operación OT, así como el reporte de la evolución en la gestión de los riesgos mencionados.

Esta guía, es la recopilación de las mejores prácticas y metodologías, en gestión de riesgos, teniendo en cuenta la importancia en la sinergia tecnológica de las organizaciones privadas y mixtas, las cuales confluyen en lo que se considera infraestructura crítica cibernética para el país.

[1] Definido por Edwards Deming es una estrategia de mejoramiento continuo dentro de un ciclo de calidad en 4 pasos a saber, Planear, Hacer, Verificar y Actuar. Tomado y traducido de *The Deming Management Method*, Mary Walton

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 relacionado 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[2] establecidos en la Ley 23 de 1982

---

[2] **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 preservativas contra actos violatorios de los derechos morales informando previamente al autor o autores para evitar duplicidad de 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 deberán ir siempre acompañados 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 ISO (International Standard Organization), 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 se ha desarrollado dentro del marco nacional establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones para facilitar la labor en la gestión de riesgos de seguridad digital que contempla las organizaciones del sector de economía privado y mixto (micro, pequeñas, medianas y grandes empresas) que deseen adoptar la guía de orientación para la gestión de riesgos de seguridad digital, promoviendo así un entorno digital seguro en todo el País, el cual permita adelantar sus actividades económicas, sociales, así como el logro de sus objetivos de una forma segura.

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.

[2] 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

Documentar y orientar a las organizaciones de los sectores de economía mixta y privado (micro, pequeñas, medianas y grandes empresas), para la implementación de la gestión de riesgos de seguridad digital conforme al Modelo de Gestión de Riesgos de Seguridad Digital MGRSD, para incrementar la confianza de las partes interesadas respecto al uso de la tecnología y del aseguramiento de los activos de información en cada una de ellas y por ende orientar a las organizaciones que apliquen la GRSD sobre sus infraestructuras criticas cibernéticas (ICC).

1.3.2 Objetivos específicos

- ✓ Generar confianza en el uso del entorno digital, creando mecanismos y condiciones que suplan la necesidad de aplicar y mantener el proceso para la gestión del riesgo de seguridad digital.
- ✓ Fomentar una disciplina para hacer de su gestión de seguridad de la información, una ventaja clave y competitiva frente a su entorno de negocio.
- ✓ Brindar una herramienta para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades, así como las potenciales oportunidades en el entorno digital.
- ✓ Generar estrategias para la implementación de planes de acción para mitigar los riesgos generados en entornos digitales y planes de acción para aprovechar las oportunidades.
- ✓ Concienciar a las organizaciones, sobre la importancia de identificar su propia infraestructura crítica cibernética y determinar si esta forma parte de la infraestructura crítica nacional.
- ✓ Sensibilizar a las partes interesadas de la organización, para que gestionen el riesgo de seguridad digital en sus actividades socioeconómicas.

1.4 Alcance de la guía

El alcance de esta guía está definido para que las organizaciones del sector de la economía privado y mixto (micro, pequeñas, medianas y grandes empresas) sean orientadas en el proceso de gestión de riesgos de seguridad digital.

1.5 Glosario

Ver Glosario en el numeral 4 del Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).

2 Justificación

Las organizaciones del sector de economía Mixto y Privado en Colombia, se ha venido apropiando de las TI, lo que significa que la seguridad digital es indispensable en el desarrollo de las actividades principales o de misión crítica del negocio, pues la confianza que generan estos sistemas hacen que sus clientes, proveedores, aliados estratégicos, entre otros, estén convencidos que los servicios prestados cuentan con las medidas de seguridad pertinentes, los cual contribuye a la economía digital del País.

El Gobierno Nacional, está empeñado en fortalecer y concienciar a las organizaciones del peligro inminente de las amenazas del ciberespacio; por tal razón el Ministerio de Tecnologías de Información y las Comunicaciones - MINTIC, pretende orientar a las empresas del sector de la economía Mixto y Privado, para que tomen conciencia, identifiquen sus activos de información, los analicen, determinen sus amenazas, vulnerabilidades y riesgos, con el fin de unificar esfuerzos, fortaleciendo el entorno digital a nivel nacional.

Esta guía se elabora con el fin de brindar orientación a las organizaciones del sector de la economía mixta y privada, permitiendo un mayor entendimiento de cada una de las fases para la implementación de la metodología de la gestión de riesgos de seguridad digital.

Antes de iniciar la implementación del modelo para la de gestión de riesgos de seguridad digital, es importante que la organización establezca claramente, el grado de madurez en que se encuentra frente a seguridad de la información, en ese sentido, la organización, podrá identificar si cuenta o no, con un sistema de gestión de riesgos para riesgos operativos (SARO), riesgos de lavado de activos y financiación de terrorismo (SARLAFT), riesgos de seguridad de la información, entre otros y armonizarlos de tal manera que se complementen con el MGRSD.

Si la organización aún no ha aplicado ningún tipo de actividad relacionada con riesgos en cualquier frente, se sugiere definir cuál de las buenas prácticas relacionadas a la gestión de riesgos se ajusta a la naturaleza de su organización, de acuerdo con la actividad propia de la misma, esta metodología deberá cubrir los aspectos de seguridad digital propuestos en el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), MAGERIT v.3:2012, la NTC (Norma Técnica Colombiana) ISO31000:2011, la norma Australiana para la gestión de riesgo, las guías de COSO ERM (Enterprise Risk Management), la NTC-ISO27005:2009, que hace referencia directamente a los riesgos de seguridad de la información, entre otros.

3 Guía para la gestión de riesgos de seguridad digital para el sector mixto y privado

En los siguientes numerales se explica paso a paso el proceso de gestión del riesgo digital, definido en el Modelo Nacional de Gestión del Riesgo de Seguridad Digital (de ahora en adelante MGRSD).

Para cada una de las fases de la gestión del riesgo digital, es necesario tener en cuenta la comunicación y la consulta y los principios fundamentales y generales, con el fin de crear las condiciones para que las múltiples partes interesadas y la ciudadanía en general, puedan gestionar los riesgos de Seguridad Digital de sus actividades económicas y sociales, fomentando la confianza en el entorno digital.

3.1 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 organización, el ecosistema digital de la organización, 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 organización deberá precisar durante la etapa de planificación:

3.1.1 Compromiso de la alta dirección

La Alta Dirección deberá 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 dicho proceso sea desarrollado de forma efectiva en la organización.

Para formalizar estos compromisos se deben documentar y mantener evidencia, que aseguren de manera permanente la designación de recursos y la inclusión de

cada uno de ellos en los espacios de seguimiento (Comités, revisiones, entre otros), que la organización tenga definidos.

3.1.2 Contexto de la organización

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

3.1.2.1 Establecimiento del contexto externo

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

- ✓ Factores del entorno cultural, político, jurídico, normativo, financiero, económico y de la competencia (si aplica), ya sea internacional, nacional, regional o local.
- ✓ Factores clave y tendencias que tengan impacto en la misión de la organización o de los objetivos trazados.
- ✓ Las capacidades y valores de las partes interesadas externas (clientes, proveedores de servicios). *Ver numeral 3.1.3 Identificación de Partes Interesadas).*
- ✓ Entes de Control, tales como superintendencias, comisiones reguladoras, entre otras.
- ✓ Clientes, Proveedores de servicios y Entidades o empresas que sean competencia directa y se relacionen con la misión de la organización analizada.
- ✓ 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 organización.

3.1.2.2 Establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- ✓ La organización en general, su funcionamiento, 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 organización y los procesos, debe considerarse, sin limitarse, los siguientes factores relacionados con el entorno digital:

Para la organización

- ✓ Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros.
- ✓ Sistemas de información o la tecnología informática que soporta las operaciones del negocio.
- ✓ Partes interesadas internas.
- ✓ Objetivos estratégicos de la organización así como 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).
- ✓ Estructura interna de la organización (organigramas, roles y responsabilidades).

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 de las actividades de gestión del riesgo
- ✓ Relaciones con otros procesos de la organización.
- ✓ Cantidad de clientes afectados por el proceso.
- ✓ Procesos de gestión de riesgos que se tienen actualmente implementados.
- ✓ Personal involucrado en la toma de decisiones.

3.1.2.3 ¿Quienes participan en el establecimiento del Contexto?

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

- ✓ Gerentes de áreas.
- ✓ Líderes de proceso.
- ✓ Líderes funcionales.
- ✓ Encargados de los sistemas de gestión.
- ✓ Encargados de los sistemas de información.
- ✓ Personal Jurídico.
- ✓ Cualquier otro rol que la Organización considere relevante.

Para la documentación de esta actividad puede utilizarse cualquier instrumento que la organización considere, donde se consigne la información recopilada durante las sesiones de trabajo. Entre éstos podrían incluirse, un documento, una matriz o un flujograma, entre otros.

3.1.3 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 Organización.
- ✓ Entidades que dependen de la generación de información de la propia Organización.
- ✓ Empresas vinculadas con la Organización.

- ✓ Personal: Funcionarios, Trabajadores, contratistas y personal de convenios.
- ✓ Medios de comunicación.
- ✓ Organizaciones nacionales e internacionales

3.1.3.1 ¿Cómo identificar las partes interesadas?

Para llevar a cabo esta actividad se sugiere hacer una lista en la que estén numeradas las partes interesadas que tengan relación con la empresa y con sus objetivos, esta se debe realizar en sesiones de trabajo donde se involucren los siguientes roles (si aplica), es aconsejable utilizar la tormenta de ideas (brainstorming)[3] o la metodología que la organización prefiera, donde todos los participantes aportarán sus ideas sobre cuáles son las partes interesadas.

- ✓ Alta gerencia.
- ✓ Gerentes de áreas.
- ✓ Líderes de proceso.
- ✓ Líderes funcionales.
- ✓ Encargados de los sistemas de gestión.
- ✓ Encargados de los sistemas de información.
- ✓ Personal Jurídico.
- ✓ Cualquier otro rol que la organización considere relevante.

Esta actividad se debe documentar y dejar un registro de la lista de las partes interesadas que se involucran con la organización y la gestión de riesgos de seguridad digital, así como la identificación de los requisitos que la organización debe tener en cuenta para satisfacer a dichas partes interesadas.

[3] Es una técnica basada en la exposición de manera informal y libre de todas las ideas en torno a un tema o problema planteado que ayuda a estimular la creatividad. http://www.kstoolkit.org/

3.1.4 Identificación de procesos donde se aplicará la gestión de riesgos de seguridad digital.

Es fundamental que la organización al desarrollar su gestión de riesgos de seguridad digital cuente con la identificación de los procesos claves que estarán dirigidos a cubrir las necesidades y expectativas de los clientes y usuarios donde se aplicará la presente guía. Por lo tanto, si la organización no cuenta con una caracterización de los procesos, entonces podría definirla teniendo en cuenta, sin limitarse, los siguientes factores:

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

3.1.4.1 ¿Cómo identificar los procesos de la organización?

Para llevar a cabo esta actividad que es de suma importancia y relevancia en una organización se debe tener en cuenta que toda la información relativa a los procesos debe ser registrada y guardada, se sugiere, para seleccionar los procesos críticos de una organización, realizar una evaluación de estos, para detectar aquellos que más fuertemente impactan en el giro de la organización, en esta selección deben participar la alta gerencia, gerentes, lideres, encargados de los sistemas de gestión entre otros, utilizando herramientas como la entrevista, lluvia de ideas, análisis de Pareto entre otros.

Para la documentación de esta actividad puede utilizarse cualquier instrumento que la organización considere, donde se consigne la información recopilada durante la sesión de trabajo. Entre estas podría incluirse, entrevistas, listas de chequeo, un documento de referencia, un diagrama de flujo, entre otros.

3.1.5 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 organización, debe tener en cuenta los lineamientos establecidos por los diferentes sistemas de gestión de riesgos ya implementados internamente, con el fin de que las políticas se armonicen en una sola incluyendo el compromiso para gestionar los riesgos de seguridad digital. De lo contrario deberá crear su propia política para la gestión de riesgos de seguridad digital. Esta actividad es responsabilidad de la alta dirección y del líder del proceso de seguridad de la información o el líder de seguridad digital.

3.1.5.1 ¿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 organización.
- ✓ Sistemas de gestión de seguridad de la información que cuente con políticas para la gestión de riesgo de seguridad digital.
- ✓ 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

queden establecidas en una política integral, en donde se evidencia también el compromiso de la organización frente a la gestión de riesgos de seguridad digital.

Cuando no se cuenta con políticas dentro de la organización:
Si la organización, aún, no cuenta con políticas de gestión de riesgo de ningún tipo, se recomienda tomar como referencia la definición de política de gestión de riesgos en el numeral 4.3.2. de la norma NTC-ISO31000:2011.

3.1.6 Definición de roles y responsabilidades

La organización 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 proceso de la organización, sin embargo se deben establecer responsables de la organización que coordinen dicha gestión.

3.1.6.1 ¿Cómo definir los Roles y Responsabilidades para la GRSD?

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

Si la organización 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.
- ✓ 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 organización 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 implementación y seguimiento de la gestión de los riesgos de seguridad digital.
- ✓ Definir el administrador para los riesgos de seguridad digital el cual se sugiere que sea el oficial es de seguridad de la información, que lidere y guíe los temas de seguridad digital y 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, objetivos y misión de la organización, 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.

3.1.7 Definición de recursos para la GRSD

La organización debe disponer de los recursos suficientes para el desarrollo de la GRSD, (capital, tiempo, persona, procesos, sistemas y tecnologías), con el fin de

ayudar a los responsables en la implementación y seguimiento de los riesgos de seguridad digital.

3.1.7.1 ¿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.
- ✓ Económicos para formar las competencias del personal, para la implementación de controles de mitigación de riesgos, aspectos de mejora continua, monitoreo y auditorías.

3.1.8 Establecimiento de criterios para evaluación de los Riesgos de Seguridad Digital

La organización debe establecer los criterios para los diferentes niveles que se definan 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.
- ✓ Del nivel de aceptación o apetito del Riesgo de Seguridad Digital.
- ✓ Las zonas de riesgo con su respectiva definición, donde se ubicarán los riesgos inherentes durante el análisis y los riesgos residuales durante su evaluación y posterior tratamiento.

La organización deberá 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, podría definir

escalas de 3, 4, 5, 6 o 7 niveles, no hay escalas obligatorias, sin embargo, para efectos de la presente guía se propone la definición de una escala de medición para el impacto, probabilidad y riesgo de seguridad digital de 5 niveles.

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

3.1.8.1 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:

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

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)**
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: Elaborado por el autor.

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

- ✓ La variable población se define teniendo en cuenta el establecimiento del contexto externo de la organización (Numeral 3.1.2), sobre el cual se está desarrollando el ejercicio ya sea por la organización del sector mixto o privado. Esto significa que para la variable "*Social*" la consideración de "*población*" va a estar asociada a los clientes/personas, a las cuales la organización les presta servicios a través del entorno digital, y que de una forma u otra podrían 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 organizaciones que la aplicarán dependen principalmente de un presupuesto para el desarrollo normal de las actividades propias de cada organización.
- ✓ Para la variable "*Ambiental*" la consideración estaría 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 organización. Es de anotar que para aquellas organizaciones 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, Hazard and Operability study (HAZOP), entre otros.

3.1.8.2 Definición de criterios de Probabilidad

La Organización puede definir escalas de medición para la probabilidad de 3, 4, 5, 6,7 niveles, según su criterio. Para las organizaciones de economía mixta o las que lo requieran, pueden utilizar como un referente la metodología de riesgos del DAFP que al igual que muchas utiliza las buenas prácticas de riesgos una escala de 5 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

3.1.8.3 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 recomendadas por esta guía y según lo dispuesto también por la Función Pública (para aquellas entidades del sector de la economía mixta), para 5 niveles de impacto y 5 niveles de probabilidad (donde 25 será el mayor valor) se consideran 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 4 y el valor de la Probabilidad es 2 el nivel de riesgo es igual a 8, lo que lo ubica en la zona de riesgo Moderado, según las zonas de riesgo de la Tabla 3.

Acción requerida: La acción requerida se refiere a que los riesgos que se ubiquen en la zona de riesgo correspondiente, deberán tomar las alternativas allí sugeridas.

No obstante las zonas al igual que los niveles de impacto y probabilidad se establecen según sea la necesidad de la organización 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.

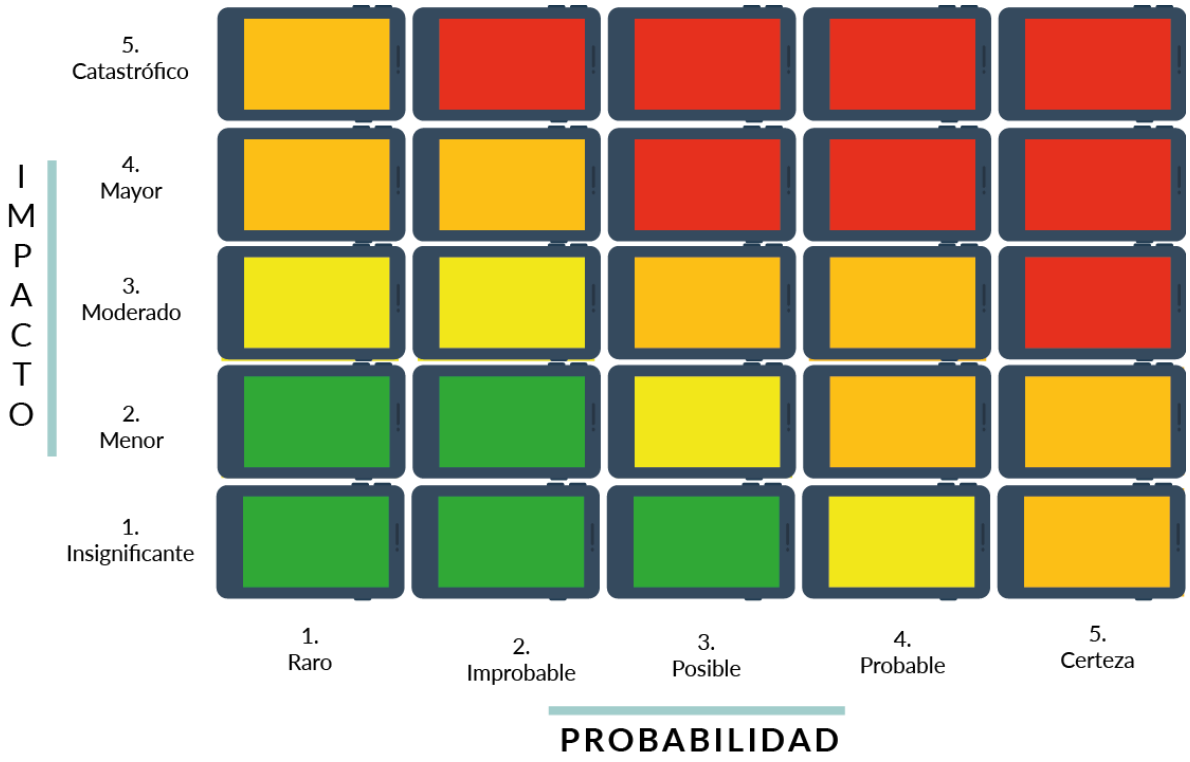

Imagen 1. Mapa de calor. Fuente el autor.

3.1.8.4 Definición de Apetito o zona de aceptación del Riesgo

El apetito de 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 organización podría definir.

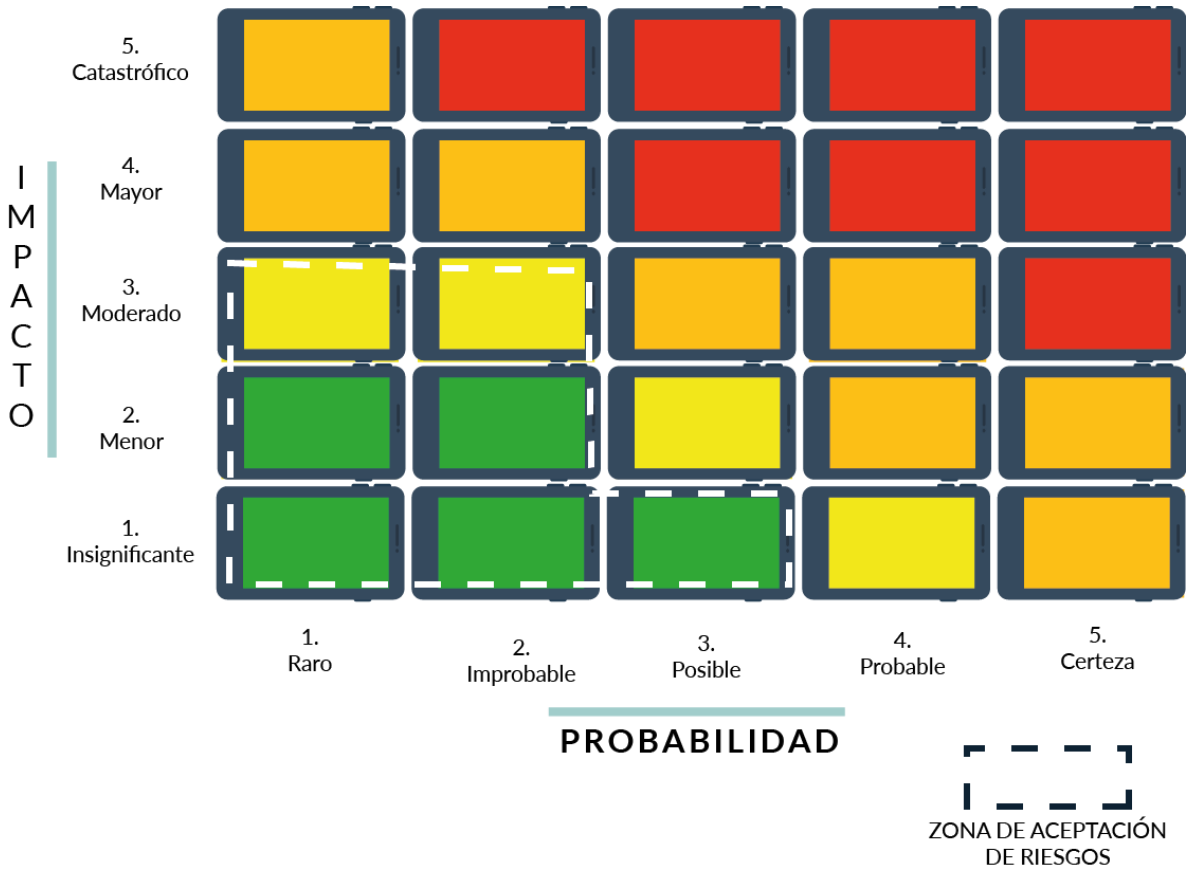

Imagen 2. Mapa de calor con definición del apetito de riesgo. Fuente el autor.

3.2 FASE 2. EJECUCIÓN DE LA GRSD

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

3.2.1 Identificación de activos de información

Para la identificación de activos de información las organizaciones de los sectores privado y mixto deberán:

- ✓ 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.
- ✓ Las organizaciones del sector de la economía mixto y privado (grandes empresas) deben Identificar si existe infraestructura crítica cibernética (ICC) e identificar activos relacionados con las tecnologías de la información de TI y con las tecnologías de operación TO asociados a la Infraestructura crítica cibernética (ICC).
- ✓ Todas las Organizaciones del sector deben clasificar la información.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

Realizar un inventario de los Activos de Información por cada proceso: Los Activos de información deberán ser identificados por medio de:

- ✓ Un consecutivo: Corresponde al número consecutivo de los activos. Por 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 organización 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 u organización 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 al tipo de activo de información, a continuación se relaciona algunos tipos de activos, sin limitarse, a los que pueda definir la organización:

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 determinar el nivel de importancia de los activos, se sugieren las siguientes premisas; sin embargo la organización 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 organización 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, las organizaciones de los sectores mixto y privados (empresas grandes) deberán determinar si los procesos en los cuáles identificó los activos de información, son servicios esenciales y si estos hacen parte de la infraestructura crítica cibernética (de ahora en adelante 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 organización cuenta con ICC deberá reportarla al CCOC.

Nota: La organización 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 las administraciones públicas".[4]

Identificar activos de TI/TO asociados a la ICC: Una vez la organización 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 organización debe tomar como referencia la "*Guía de ICC de acuerdo al 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 a tomar como referencia, está determinada por la misión de cada organización, puede per tener a los 13 sectores descritos en el Modelo Nacional de Gestión de Riesgos "Numeral 3, literal b".

Clasificar la información: La organización deberá clasificar sus activos de información identificados, incluyendo los activos de Infraestructura Crítica cibernética, de acuerdo a las políticas establecidas por cada una de ellas o tomando como referencia lo definido a continuación.

Para las organizaciones de economía mixta se debe clasificar las información de acuerdo a la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional Ley 1712:2014 (Las personas naturales y jurídicas, públicas o privadas, que presten función pública) principalmente relacionando el artículo n°6.

Tabla 6. Clasificación de la información

Tipos de clasificación	Descripción

[4] Tomado de la "guía para la Identificación de Infraestructura Crítica Cibernética de Colombia Primera Edición" emitida por el Comando Conjunto Cibernético (CCOC)

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

3.2.2 Identificar los riesgos inherentes de seguridad digital

Los riesgos se deberán 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 habría que tenerse 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
	Fallas en el sistema de suministro de agua	E

Pérdidas de los servicios esenciales	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, 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 organización 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.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

Identificación de vulnerabilidades: La organización puede identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización de la organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal.
- ✓ Ambiente físico.
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.
- ✓ 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 al tipo de activos y sus 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 organización 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.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

Identificación del riesgo inherente de seguridad digital: Para cada tipo de activo hay una serie de riesgos, los cuales la organización debe identificar. A continuación se relacionan ejemplos de riesgos con sus respectivas amenazas y vulnerabilidades de acuerdo al 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 que situaciones adversas asociadas al manejo de la información digital y los activos de información se podrían presentar, casos ocurridos que los participantes conozcan que se hayan dado en la organización o en el sector. Debe existir un orden de la sesión, un líder de la misma y personas que ayuden con captura de las memorias.
- ✓ **Juicio de expertos:** a través de este esquema, se reúnen las personas con mayor conocimiento del entorno materia de análisis e indican de aspectos negativos o riesgos de seguridad digital que se podrían llegar a 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 retomarán los principales riesgos identificados y se puede proceder a una valoración de los mismos.

- ✓ **Análisis de escenarios:** Bajo este esquema, también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que podrían llegar a presentarse: Explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente, con base en ello, se determina que podría llegar a suceder desde la perspectiva digital a los activos de información o como consecuencia de afectación de los mismos.
- ✓ **Otras técnicas que pueden ser empleadas son**: Entrevistas estructuradas, encuestas, listas de chequeo.

Nota: Si la organización 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.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

3.2.3 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 organización, el tipo de activo y de la pertinencia que tenga cada variable en la medición del Impacto.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

3.2.3.1 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 tomando como base los criterios definidos en la fase de planificación.

Para el caso del impacto es claro que se definieron 5 niveles asignados (insignificante, menor, moderado, mayor y catastrófico) para 6 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 lo mencionamos anteriormente (ver nota del numeral 4.2.3), no necesariamente aplica a todas las 6 variables. Por lo tanto, se deben considerar solamente aquellas que realmente apliquen para el análisis. El impacto total, podrá 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 Organización del sector privado 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 3.

- ✓ **Impacto:** Según análisis de la información realizada por el experto de la organización, 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 4 variables únicamente. De acuerdo con lo anterior, la organización puede calcular las variables para las cuales tienen información o son relevantes dentro del proceso o activo evaluado.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

- ✓ **Análisis:** El experto que analiza esta situación, al obtener el promedio de estas 4 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 3 y el Impacto es 2. A continuación se presenta el ejemplo de ubicación del riesgo.

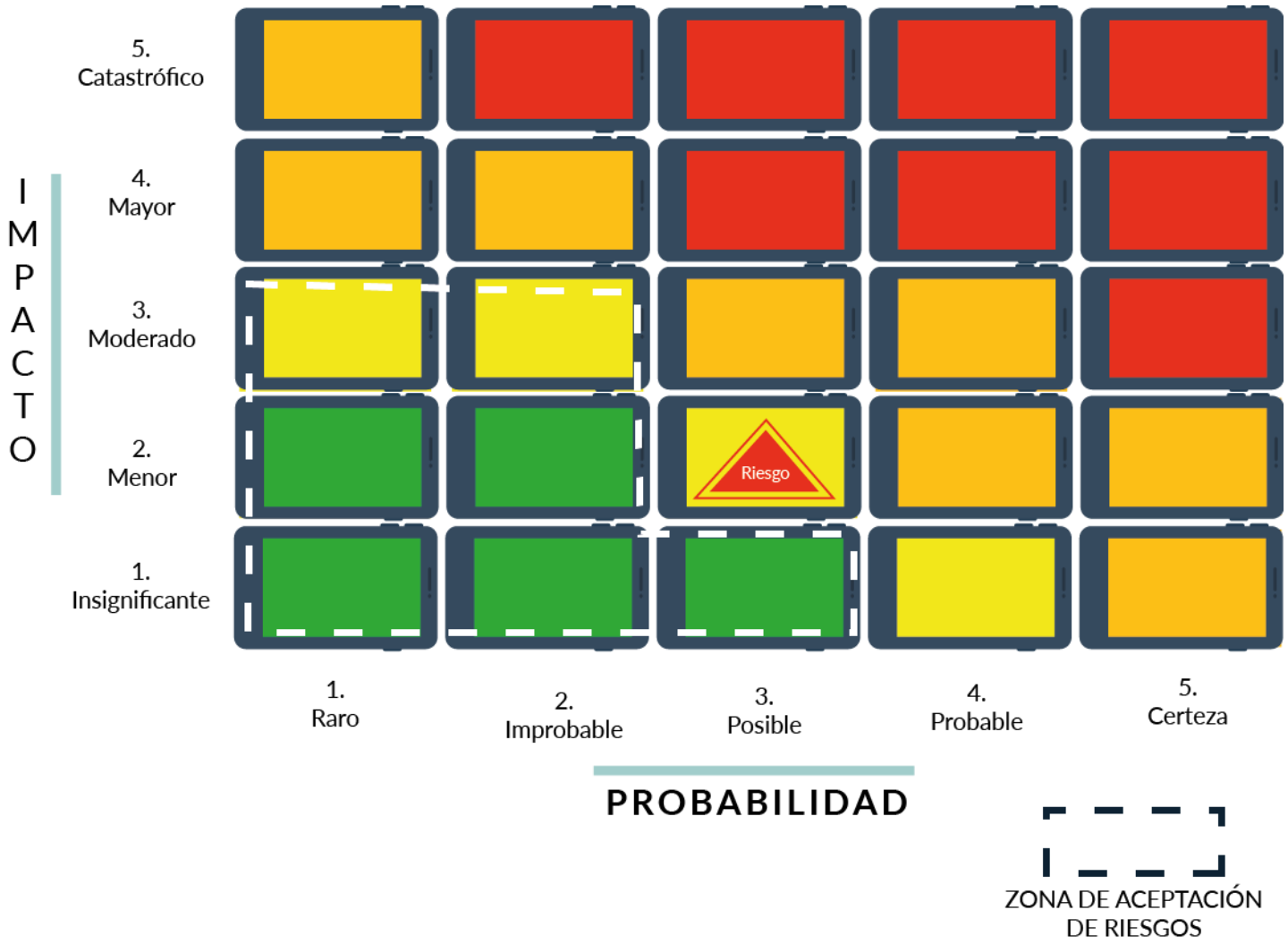

Imagen 3. Ejemplo determinación probabilidad de ocurrencia e impacto. Fuente el autor.

3.2.4 Identificación y evaluación de los controles

Una vez identificado los riesgos inherentes se procede a la identificación y evaluación de los controles.

Para las organizaciones de economía mixta o las que lo requieran, pueden utilizar como un referente la metodología de riesgos para ello se puede tomar como referencia lo definido en la guía para la Administración del Riesgo de la Función Pública[5] o lo establecido a continuación:

Notas importantes:

- 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 su evaluación en cuanto a las características de dichos 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[6]?	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

[5] Para la evaluación de controles puede tener en cuenta lo definido en la Guía para la Administración del Riesgo de la Función Pública pág. 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.

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

Fuente: elaborado por el autor

Características de controles: A continuación se presentan algunas características de los controles a manera de ejemplo. La organización 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*. **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 organización identifique los controles debe realizar un análisis de éstos, teniendo en cuenta sus características, con el fin de determinar su grado de efectividad el cual se verá reflejado con desplazamiento del riesgo dentro del mapa de calor.

Por ejemplo:

Para mayor entendimiento de esta actividad y continuando con el ejemplo anterior, a continuación se ponderan las características de tres controles asociados al riesgo de "acceso no autorizado a una base de datos". Si la organización aún no ha valorados los controles, puede seguir este ejemplo o si es una organización del sector mixto, puede tomar como referencia lo definido en la Guía para la administración del riesgo de la Función Pública - DAFP. Los controles se evalúan acorde a 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
	Documentación	Sí existe = 1 No existe = 0	1	0	0
Control 2. El uso de una herramienta automática que registra las	Complejidad	Complejo para ejecutar = 1 No complejo = 0	1	0	0
	Responsable del control	Asignado = 1 No asignado = 0	1	0	0

transacciones que este administrador realiza.	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 **10**, valor que debe ser comparado con los rangos de la tabla a continuación, que 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 acabamos de evaluar, el control resulto efectivo, pero solamente se desplazará en probabilidad y no en impacto, dado que el promedio de las características mencionadas en el criterio de desplazamiento establece que el promedio de “podría disminuir la probabilidad” es 0,66 y el promedio de “podría disminuir el impacto” es 0,33, lo cual según los criterios sólo desplaza hacia la izquierda un cuadrante.

Nota: Si la organización 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.

Nota: En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta identificación de activos como lo sugieren metodologías tales como NTC ISO 27005:2011, MAGERIT V3: 2012, en el submodelo de elementos que hace referencia a los activos de información.

3.2.5 Determinación del riesgo residual

Una vez evaluados los controles, se calculó de acuerdo al 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 que es efectivo y que 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).

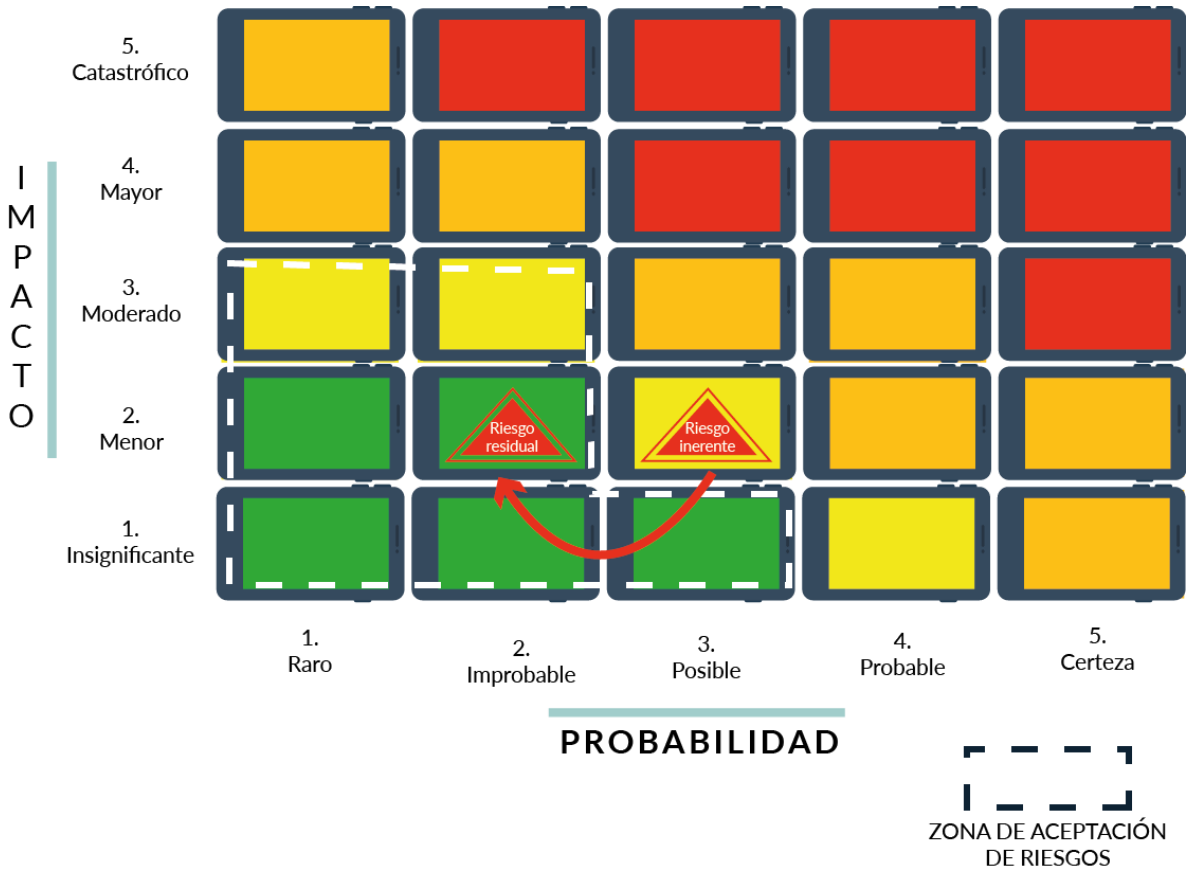

Imagen 4. Determinación del riesgo residual. Fuente el autor.

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"

3.2.6 Tratamiento de los riesgos de seguridad digital

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

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 organización puede tener en cuenta las siguientes opciones:

- ✓ **Evitar el riesgo:** La organización 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, deberían ser adoptados de igual forma aunque monitoreados para evitar que se aumenten sus niveles ya sea de probabilidad o de impacto.

- ✓ **Transferir el riesgo:** Si la organización no pudiere o no desea asumir la gestión del riesgo, entonces podría transferirlo a terceros o compartirlo con otra organización.

- ✓ **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 organización 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 podría suponer una situación en donde la organización no puede costear una aplicación para registrar las actividades del administrador de Base de datos (Control 2 propuesto). Por lo tanto, la organización 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 organización deberá definir las acciones a seguir para priorizar los tratamientos de acuerdo al impacto del riesgo residual, para ello 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 organización 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 organización deberá hacer un seguimiento al plan de tratamiento para determinar su efectividad, de acuerdo a 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: Después que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos prevista, la organización debe valorar nuevamente el riesgo y verificar si el nivel de dicho riesgo disminuyó o no (es decir se desplazó de una zona mayor a una menor en el mapa de calor), comparándolo con el último nivel de riesgo residual.

3.3 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 a lo definido por la organización, 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.

3.3.1 Registro y reporte de eventos de riesgos de seguridad digital

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

3.3.1.1 Reporte de la gestión del riesgo de seguridad digital al interior de la organización

La organización debe reportar periódicamente a la Alta Dirección y a las partes interesadas la siguiente información:

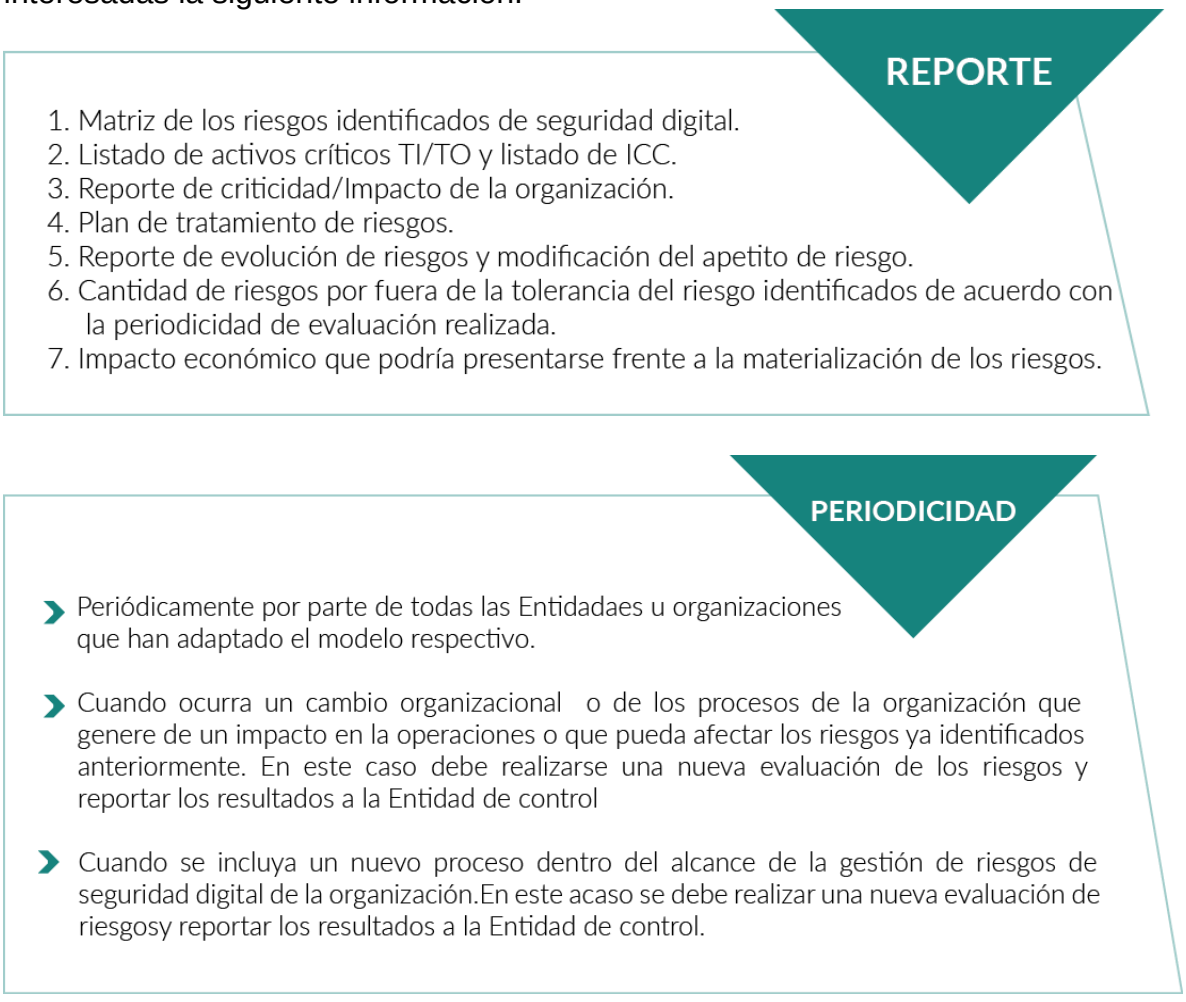

Imagen 1. Reporte de información por parte de la entidad. Fuente: MinTIC

3.3.1.2 Reporte de la gestión del riesgo de seguridad digital

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.

Reportes a entidades de interés especial, si se es entidad privada:

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 a la alta dirección de la entidad para la debida gestión interna y a los CSIRT Sectoriales una vez estos se hayan creado.

Reportes a entidades de interés especial, 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 vulnerabilidad críticas relacionados con estas, deberán reportarse al CCOC, dado que es la entidad encargada de administrar esta información.

Nota 1: Los reportes de información a las entidades de interés especial, definidos para las entidades privadas, se plantean como ejercicio colaborativo voluntario en el fortalecimiento de la seguridad digital del país.

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).

Nota 3: para implementar estas actividades, se establece el numeral 4.3. Fase 3. Monitoreo y Revisión, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como las entidades correspondientes a la fuerza pública).

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.

3.3.2 Auditorías internas y externas.

Deben programarse y ejecutar auditorías [7] internas y externas con fechas planificadas, las cuales deben quedar registradas en el plan anual de auditoría.

3.3.3 Revisión por parte de la Alta Dirección

La Alta Dirección de la organización debe realizar revisiones periódicas y el respectivo seguimiento al proceso de gestión de riesgo de seguridad digital.

[7] 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*" de MINTIC, estrategia Gobierno en Línea (GEL).

3.3.4 Medición del desempeño

La organización debe utilizar medidas de desempeño[8] para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente.

3.3.5 Rendición de cuentas

Las múltiples partes interesadas deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones. También deben reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales[9].

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

La organización debe propender por la mejora continua[10] de la gestión de riesgos de seguridad digital, por lo tanto debe establecer que:

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

b. 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.

[8] 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*" de MINTIC, estrategia Gobierno en Línea (GEL).
[9] Tomado del CONPES 3854
[10] 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).

- ✓ Determinar si existen otras no conformidades similares para establecer acciones correctivas evitando así que éstas lleguen a materializarse.
- ✓ Emprender acciones detectivas que permitan gestionar el riesgo a tiempo, disminuyendo 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 de ésta y su resultado, para futuras no conformidades.

3.4.1 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.

3.4.1.1 ¿Cómo realizar la Comunicación y Consulta?

Para la ejecución de esta fase, la organización debe establecer o asegurarse que se cuente con un plan de comunicación, el cual especifique como mínimo lo siguiente:

- ✓ 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