

Evaluación y tratamiento del riesgo

**Breve descripción:**

La evaluación y el tratamiento del riesgo es responsabilidad de todo funcionario comprometido con el mejoramiento continuo de la organización y la prevención de sucesos que pueden afectar su normal funcionamiento. El análisis del riesgo tiene como objetivo evitar grandes inversiones de recursos en la gestión interna para superar eventos correctivos que afecten la productividad, enfocando. esfuerzos en la eficiencia de las **Área ocupacional:**

Administración y finanzas

**Junio 2024**

Tabla de contenido

[Introducción 3](#_Toc169203621)

[1. Evaluación del riesgo 5](#_Toc169203622)

[1.1 Riesgo empresarial 8](#_Toc169203623)

[1.2 Determinación de ocurrencia 13](#_Toc169203624)

[1.3 Modelos de estimación 16](#_Toc169203625)

[1.4 Mapa de riesgos 18](#_Toc169203626)

[1.5 Tratamiento de riesgos 21](#_Toc169203627)

[1.6 Normativa técnica 25](#_Toc169203628)

[2. Gestión de la información 29](#_Toc169203629)

[2.1 Protocolos de elaboración 32](#_Toc169203630)

[2.2 Normativa de protección de datos 36](#_Toc169203631)

[Síntesis 43](#_Toc169203632)

[Material complementario 45](#_Toc169203633)

[Glosario 47](#_Toc169203634)

[Referencias bibliográficas 48](#_Toc169203635)

[Créditos 49](#_Toc169203636)

Introducción

Como bienvenida al presente componente formativo, que expone el análisis de la evaluación y tratamiento del riesgo como elemento fundamental para el normal funcionamiento y la mejora continua de las organizaciones, se presenta el siguiente video introductorio:

1. Evaluación y tratamiento del riesgo



[**Enlace de reproducción del video**](https://youtu.be/6kk2Bna8lZg)

|  |
| --- |
| **Síntesis del video: Evaluación y tratamiento del riesgo** |
| Un sistema de gestión contempla todas las políticas, la información, los recursos y las normas de una entidad, buscando resultados que satisfagan las necesidades de productividad en un marco de integridad, transparencia y legalidad.  Los sistemas de gestión se complementan e integran con otros modelos, sistemas o estrategias estableciendo directrices de desempeño y gestión para las empresas referentes para la planeación, la dirección, la ejecución, el seguimiento, la evaluación y el control de procesos.  Todo riesgo tiene un ciclo que inicia con la identificación y modelamiento de factores de riesgo, pasando por el diseño e implementación de estrategias y el seguimiento, etapa indispensable en la toma de medidas que eviten una repetición eventual del riesgo.  La ausencia de una gestión del riesgo eficiente desencadenaría una serie de eventos desafortunados, llevando a la empresa al deterioro de sus indicadores de gestión, financieros y operativos, traducidos en bajos niveles de inversión y flujos de caja, pérdida de capital humano, baja productividad y eficiencia en sus operaciones.  Es por ello, que existen premisas a tener en cuenta para gestionar los riesgos en las empresas:   * Es imposible eliminar el riesgo. * Es mejor prevenir que lamentar. * El riesgo se gestiona en términos de probabilidad. * Es mejor ser aproximadamente oportuno que exactamente inoportuno. * Evitar el miedo al arrepentimiento. * Considerar los riesgos geográficos interrelacionados.   La Norma ISO 31000 contempla herramientas y técnicas para la gestión de riesgos dentro de las que se destacan los tipos de riesgos empresariales y las directrices, las metodologías y los procesos de gestión, el plan de tratamiento, las rutas de atención y los parámetros de criticidad, los métodos de medición de probabilidades y la técnica de elaboración de la matriz de riesgos, el riesgo empresarial, los riesgos sistemáticos y no sistemáticos, la teoría de probabilidades y el análisis de incertidumbre, el diseño de modelos de estimación, la gestión de la información y la evaluación, el diseño e implementación de los sistemas de gestión. |

# Evaluación del riesgo

Dirigir una compañía implica, en un alto grado de responsabilidad, la gestión y evaluación adecuada de los riesgos a los que se expone a diario la empresa. Dichos riesgos pueden ser internos y externos.

**Riesgos internos**

Operaciones, recurso humano, instalaciones.

**Riesgos externos**

Inflación, interés, políticas, tasa de cambio, desempleo, riesgo del país.

Según la Norma ISO 31000-2018 el proceso de evaluación de los riesgos consta de cuatro pasos básicos: **identificación, análisis, valoración y tratamiento** de los riesgos, que dejan a disposición de la empresa una amplia gama de técnicas para identificar la incertidumbre que puede llegar a afectar a uno o a varios de sus objetivos. A continuación, se describen los cuatro pasos mencionados:

1. **Identificación de riesgos**

**Propósito**: detectar, inspeccionar y explicar los riesgos que pueden obstaculizar a una empresa en el logro de sus objetivos.

**Importante**: contar con información actualizada, oportuna y adecuada que permita caracterizar los riesgos y sus niveles de impacto.

**Factores a considerar**:

* Fuentes de riesgo tangibles e intangibles.
* Causas y eventos.
* Amenazas y oportunidades.
* Vulnerabilidades y capacidades.
* Cambios en los contextos externo e interno.
* Indicadores de los riesgos emergentes.
* Naturaleza y valor de activos y recursos.
* Consecuencias y sus impactos en los objetivos.
* Limitaciones de conocimiento y la confiabilidad de la información.
* Factores relacionados con el tiempo.
* Sesgos, supuestos y creencias de las personas involucradas.

1. **Análisis de riesgos**

Se realiza con diferentes grados de complejidad, todo depende de su propósito, la disponibilidad, la transparencia y la confiabilidad de la información y de los recursos disponibles.

Utiliza técnicas que pueden variar entre cualitativas, cuantitativas o mixtas.

**Factores a considerar**:

* Probabilidad de eventos y consecuencias.
* Naturaleza y magnitud de las consecuencias.
* Complejidad e interconexión.
* Factores relacionados con el tiempo y la volatilidad.
* Eficacia de controles existentes.
* Niveles de sensibilidad y de confianza.

1. **Valoración de riesgos**

**Propósito**: apoyar en la toma de decisiones, lo que implica comparar resultados del análisis del riesgo para determinar en qué momento se requiere una acción adicional.

**Decisiones que se pueden abordar en la valoración de riesgos**:

* No hacer nada más.
* Considerar opciones para el tratamiento del riesgo.
* Realizar un análisis adicional para comprender mejor el riesgo.
* Mantener controles existentes.
* Reconsiderar objetivos.

1. **Tratamiento de riesgos**

* Supone hacer una evaluación de los beneficios/costos derivados de la consecución de los objetivos.
* Procesos interactivos a ejecutar en el tratamiento de los riesgos:
* Formular y seleccionar opciones para el tratamiento del riesgo.
* Planificar e implementar el tratamiento del riesgo.
* Evaluar la eficacia de ese tratamiento.
* Decidir si el riesgo residual es aceptable.
* Si no es aceptable, efectuar tratamiento adicional.

En las empresas es primordial contar con un plan adecuado de prevención y evaluación de riesgos, que permita realizar un diagnóstico acertado y conocer de manera anticipada los sucesos internos o externos que puedan afectar el normal funcionamiento de la compañía. Con base en ello, se ejecutan acciones para minimizar o trasladar el riesgo, así la empresa sería capaz de afrontar sin mayores contratiempos, las consecuencias o pérdidas al materializarse el riesgo (Cristo, 2019).

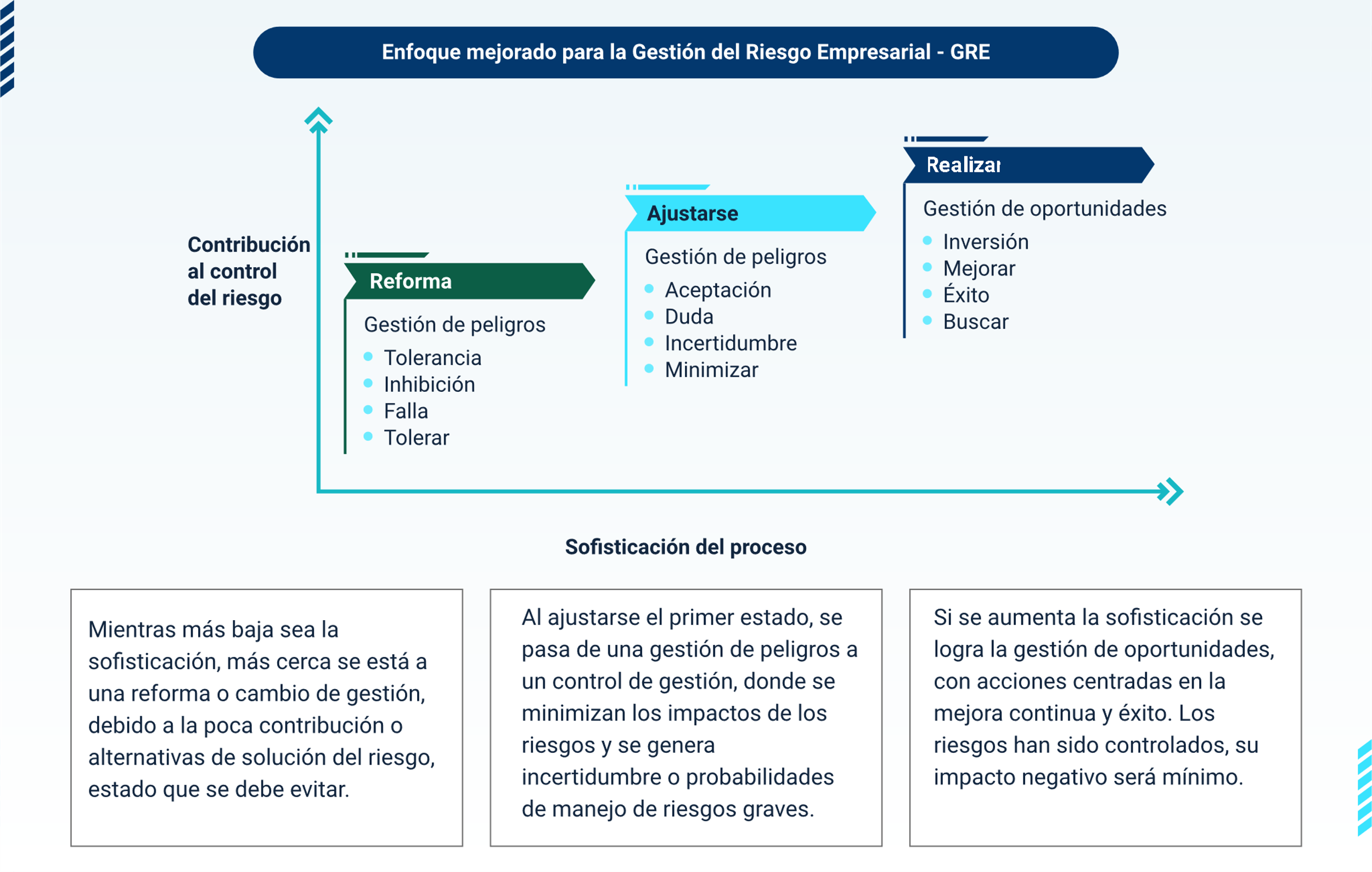
## 1.1 Riesgo empresarial

La gestión del riesgo empresarial - GRE afecta a los órganos directivos y laborales de la organización (junta directiva, administrativos y empleados) y se diseñó para perfilar eventos que puedan impactar a la entidad, de forma que el riesgo este en el rango de impacto deseable y razonable que no afecte los objetivos de la organización.

La GRE debe impactar en todos los niveles e incluirse en los modelos de la estrategia organizacional, con el fin de identificar alternativas de solución preventivas y no correctivas enfocadas siempre al cumplimiento de metas, independientemente del departamento al cual se esté aplicando la estrategia.

El siguiente esquema presenta el nivel de sofisticación en la gestión el riesgo:

1. Sofisticación del riesgo.



Nota. Adaptado de Risk likelihood and magnitude, Hopkin (2010).

**Enfoque mejorado para la gestión del riesgo empresarial - GRE**

**Contribución al control del riesgo:**

**Reforma:**

Gestión de peligros

* Tolerancia.
* Inhibición.
* Falla.
* Tolerar.

**Ajustarse**

Gestión de peligros

* Aceptación.
* Duda.
* Incertidumbre.
* Minimizar.

**Realizar**

**Gestión de oportunidades**

* Inversión.
* Mejorar.
* Éxito.
* Buscar.

**Sofisticación del proceso**

Mientras más baja sea la sofisticación, más cerca se está a una reforma o cambio de gestión, debido a la poca contribución o alternativas de solución de riesgo, estado que se debe evitar.

Al ajustarse el primer estado, se pasa a una gestión de peligro a un control de gestión, donde se minimizan los impactos de los riesgos y se genera incertidumbre o probabilidades de manejo de riesgos graves.

Si se aumenta la sofisticación, se logra la gestión de oportunidades con acciones centradas en la mejora continúa y éxito. Los riesgos han sido controlados, su impacto negativo será mínimo.

**Clasificación de riesgos empresariales**

En el siguiente recurso se presentan dos tipos de riesgo, según su impacto o según la posibilidad de prevenirlos o no:

**Cisne blanco**

Riesgos fácilmente cuantificables y sujetos a la "ley de grandes números" y reversión media.

Se prestan fácilmente al modelo probabilístico, usando como base datos históricos o utilizando el conocimiento basado en la experiencia compartida dentro de la organización.

**Cisne negro**

De naturaleza impredecible, singulares, de alta volatilidad y un impacto potencialmente cambiante.

No se puede aplicar el modelado probabilístico. Ante este tipo de evento el manejo del riesgo se hace indispensable para asegurar la supervivencia empresarial.

**Tipos de riesgos y naturaleza**

La forma más eficiente de incrementar o cumplir las metas establecidas es tener siempre presente que existen riesgos que pueden afectar la situación. Antes de definir cualquier estrategia de gestión de riesgos es necesario analizar los posibles riesgos y clasificarlos así:

* **Riesgo sistemático**: integra los elementos socio-político-económicos que afectan el normal funcionamiento de un proyecto o empresa, por ejemplo, crisis financieras, guerras, desplazamientos, entre otros.
* **Riesgo no sistemático**: afecta de manera específica un proyecto o empresa, por ejemplo, mala estrategia de gerencia, mal funcionamiento de una maquinaria, empleados inconformes, entre otros.

## 1.2 Determinación de ocurrencia

El análisis de los riesgos permite recopilar la información del sistema y de los procesos que se utilizan en las empresas para mejorar el uso, la manipulación, la protección y la administración de los recursos ante las vulnerabilidades que se pudiesen encontrar. Por tal motivo, es indispensable hacer control a la probabilidad de ocurrencia de los eventos y sus posibles consecuencias.

Existen diversas formas de gestionar un análisis de riesgos, lo más importante es conocer o entender la forma en que se determinará el valor del riesgo. Una forma sería multiplicar la vulnerabilidad por el % de importancia o peso para la empresa, es decir, mientras más vulnerable sea un activo y más importante sea este para la entidad, mayor será su riesgo. Por lo tanto, la inversión en tiempo, dinero o mano de obra será mayor para lograr minimizarlo.

El riesgo concierne a situaciones donde las probabilidades de resultados y sus consecuencias se determinan con técnicas de datos reales, completos y verídicos. Por otro lado, la incertidumbre ocurre cuando los datos utilizados presentan fragmentación, registros incompletos o datos no disponibles.

**Teoría de probabilidades**

Es una herramienta que establece un conjunto de reglas o principios para calcular la ocurrencia de los eventos, asignando un número a la posibilidad de que un evento ocurra. Aproxímese al concepto de teoría de probabilidades a través del siguiente video:

1. Teoría de probabilidades



[**Enlace de reproducción del video**](https://youtu.be/8CE3TX-rJnw)

|  |
| --- |
| **Síntesis del video: Teoría de probabilidades** |
| La probabilidad de un suceso está comprendida como un número real en el rango (0, 1), su notación viene dada por P(A), donde P es la probabilidad, A es el suceso o evento. Se lee la probabilidad del evento A y representa la frecuencia con la que se observa la ocurrencia del evento A, al efectuarse un estudio de eventos aleatorios.  El objetivo de la teoría de la probabilidad aplicada a la gestión de riesgos es el de suministrar un modelo matemático eficiente y adecuado que se pueda aplicar en la descripción e interpretación de los riesgos aleatorios, donde P(A) es la probabilidad de que A ocurra, P (A´) es la probabilidad de que A´ no ocurra y su suma igual al 100 % ó 1.  Así en el caso de una moneda, se sabe que al tirarla sobre un tablero el resultado puede ser cara o sello, suponiendo que la moneda y el tablero son perfectos y que las condiciones del lanzamiento no cambian, la probabilidad ser de 50 % cara y 50% sello. En este punto nace el concepto de probabilidad, entendida como un número entre 0 y 1, habitualmente expresado en porcentaje entre 0 y 100, que dice en cuantas ocasiones de media ocurrirá un suceso cada 100 veces.  La teoría de la probabilidad se encarga de estudiar que número entre 0 y 1 se debe asignar a un determinado suceso, es decir, estudia las probabilidades de que un evento suceda o no. |

**Análisis de incertidumbre**

* **Resultados conocidos**

Los posibles resultados que pueden obtenerse son conocidos a “priori”.

* **Probabilidades**

Análisis de probabilidades de cada opción. Medir el resultado.

* **Evaluación y cálculo**

Apuesta de forma analítica por una opción u otra, con base en información.

* **Efectos posibles**

Valoración de efectos posibles con conciencia que pueden producir efectos no esperados.

* **Posibilidades**

La incertidumbre no se puede medir de forma controlada. Solo se valoran opciones.

* **Intuición y experiencia**

Se trata de mejorar posibilidades actuando de forma intuitiva.

**Importante**

* Se debe afrontar la incertidumbre ejerciendo influencia en las situaciones deseadas, en lo que se quiera que ocurra.
* Se deben enfocar los esfuerzos en obtener una alta probabilidad de conseguir los resultados deseados, a pesar de la incertidumbre.
* No se pueden afrontar las situaciones intentando conseguir algo en concreto, sino buscando aumentar las probabilidades de que eso en concreto suceda.
* No se puede eliminar del todo la incertidumbre, pero sí tratar de inclinar la

balanza a favor.

## 1.3 Modelos de estimación

En el campo de los riesgos previsibles, la estimación trata de valorar la probabilidad de ocurrencia y el nivel de impacto de los riesgos que se componen y que, teniendo en cuenta su materialidad, requieren una valoración y presentan unos niveles de asignación. La asignación distribuye los riesgos según la capacidad de gestión, para que puedan controlase, administrarse y mitigarse. La valoración determina la estimación que puede ser cualitativa o cuantitativa, tal y como se detalla a continuación:

* **Estimación cualitativa**

Riesgos estructurados por rangos que permitan clasificarlos y calificarlos en una matriz con diversos niveles de probabilidad e impacto de ocurrencia de un evento que pueda afectar de manera desfavorable y significativa el normal desarrollo del proyecto, donde se debe tener en cuenta lo siguiente:

* + Según la experiencia en proyectos de objetos similares y datos históricos relacionados con el factor de riesgo que se va evaluar, se puede inferir su comportamiento futuro y cuantificar las posibles consecuencias del riesgo.
  + Teniendo en cuenta la evidencia empírica y las prácticas en el sector dentro del cual se desarrolla el proyecto, se puede asignar un valor numérico tanto a la probabilidad como al impacto de los riesgos previamente cualificados.
  + Se puede recurrir a publicaciones y estudios técnicos que proponen modelos y procedimientos para valorar ciertas clases de riesgos.
  + Se puede utilizar la herramienta de valoración de riesgos que proporciona una aproximación general del valor de su riesgo.
  + Se puede recurrir a las opiniones de expertos, con el fin de que emitan conceptos relacionados con la cuantificación de las posibles consecuencias económicas que tendría la ocurrencia de un riesgo determinado.
* **Estimación cuantitativa**

Se realiza después de la estimación cualitativa, con la integración de sus criterios a través de una aproximación numérica que valora el impacto de los riesgos previamente identificados, teniendo en cuenta:

* El tipo y la modalidad del proyecto son relevantes para la determinación del nivel de transferencia de las responsabilidades.
* La transferencia de los riesgos debe ser proporcional a la cantidad de información con la que se cuente para su mitigación.
* La asignación de los riesgos previsibles, atendiendo a las capacidades de los contratistas para su administración y a la existencia en el mercado de garantías que constituyan el soporte o el respaldo financiero o asegurador del proyecto.
* El traslado del riesgo no tiene connotaciones infinitas.

Es importante poder cuantificar y categorizar los riesgos, porque de acuerdo con su nivel o puntaje de evaluación o estimación se logran jerarquizar a través de un plan de acción o intervención, tratando siempre de actuar sobre aquellos que son más críticos y pueden llegar a ser más perjudiciales para el normal desarrollo de un proyecto o funcionamiento de una empresa. Estos niveles jerarquizados se plasman para una mejor lectura y comprensión en un mapa de riesgos.

## 1.4 Mapa de riesgos

Identifica de forma gráfica los riesgos a los que se expone una empresa, teniendo en cuenta su probabilidad y el impacto que pueden causar.

**Importante**

* Compartir y recopilar información de manera clara posibilita reconocer con rapidez los riesgos y actuar de acuerdo con su nivel de importancia.
* Identificar los riesgos de forma correcta permite establecer niveles en diferentes áreas de la empresa, lo que conlleva a establecer el objetivo del mapa de riesgos.

**Pasos para elaborar un mapa de riesgos**

La secuencia ofrecida a continuación detalla los pasos recomendados para la elaboración de un mapa de riesgos:

**Paso 1. ¿Qué es el riesgo?**

Obtener una definición clara y consistente de lo que es el riesgo.

**Paso 2. Metodología**

Adoptar una metodología común para evaluar la importancia del riesgo.

**Paso 3. Alcance**

Limitar el alcance de la investigación de riesgos.

**Paso 4. Actividades**

Identificar las principales actividades de la organización.

**Paso 5. Identificación de riesgos**

Identificar los riesgos que pueden afectar a esas actividades.

**Paso 6. Evaluación de riesgos**

Evaluar los riesgos con y sin acciones para minimizar el impacto o la probabilidad.

**Paso 7. Tratamientos**

Identificar los posibles tratamientos a implementar para reducir el impacto o la probabilidad.

Los mapas de riesgos se deben revisar periódicamente, teniendo en cuenta que la gestión y los riesgos son dinámicos, es decir, lo que hoy se puede identificar como un peligro, a futuro puede no existir o transformarse en una oportunidad y viceversa. Por eso, el mapa de riesgos debe pasar por revisiones según los cambios o entorno de la empresa, aunque algunas no tienen mayores alteraciones, otras entidades proclives a cambios constantes.

Es importante recordar que dentro de las **técnicas de elaboración de un mapa de riesgos** se destacan las siguientes:

1. **Nombrar un comité de riesgo**

Identificar las situaciones o riesgos que pongan en peligro el funcionamiento de un proyecto o empresa es responsabilidad de la alta gerencia; por ello, el gerente debe conformar un equipo multidisciplinar que pueda identificar los riesgos.

1. **Definir qué es un riesgo**

El comité debe recopilar toda la información necesaria y definir para la organización o para el proyecto ¿qué es un riesgo? El riesgo ayuda a controlar las crisis anticipándose a lo que pueda ocurrir.

1. **Identificar riesgos**

El trabajo en equipo se ve reflejado en el momento que cada responsable de área analice los procesos e identifique los riesgos propios de su área (esas situaciones que afectan el desempeño normal de las actividades). Identificados los riesgos se realiza un inventario o lista, con su descripción para conocer las posibles consecuencias.

1. **Valorar los riesgos**

El equipo debe clasificar los riesgos, teniendo en cuenta la caracterización realizada en el paso anterior. A continuación, se debe establecer un nivel de riesgo (alto, medio o bajo) y las acciones que se van a implementar. También se define si el riesgo es sistemático o no sistemático

1. **Matriz de priorización**

De acuerdo con la valoración de riesgos obtenida se elabora una matriz de priorización que permite establecer qué riesgos necesitan atención inmediata. Se analiza el riesgo y se clasifica como:

* **Alto**. Es muy probable que ocurra.
* **Medio**. Puede ocurrir.
* **Bajo**. Muy poco probable que ocurra o improbable.

**Nota**. El mapa de calor de riesgo consiste en una matriz con dos ejes, el Y representa la probabilidad de frecuencia del riesgo y el eje X, el impacto que puede tener. Tomado de Mapa de calor, Londoño (2020).

## 1.5 Tratamiento de riesgos

Está basado en el diseño, la evaluación, la selección e implementación de acciones para plantear los riesgos identificados al interior de una empresa. Según la norma internacional ISO 31000 el tratamiento de riesgos es un proceso cambiante y repetitivo que requiere de actividades de formulación, planeación y evaluación, tales como:

* Formular opciones para el tratamiento de riesgos.
* Seleccionar la opción más adecuada.
* Planificar e implementar el tratamiento de riesgos.
* Evaluar la efectividad de las acciones implementadas.
* Calificar el riesgo residual (aceptable o no aceptable).
* Tratamiento para el riesgo residual no aceptable.

Las opciones del tratamiento de riesgo resultan más efectivas cuando se ponen en una balanza los beneficios y los costos. Los beneficios procedentes de la efectividad de una acción propuesta y los costos del esfuerzo y las desventajas que casualmente surjan como consecuencia de la implementación. Según la Norma ISO 31000 las opciones de tratamiento no son excluyentes entre sí e incluyen algunas de las siguientes acciones:

* Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
* Asumir el riesgo, aún aumentándolo, con el fin de incrementar una posible oportunidad.
* Tomar acciones para disminuir la probabilidad del riesgo.
* Implementar acciones que disminuyan el impacto negativo del riesgo.
* Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros).
* Retener el riesgo con base en información confiable.

La implementación de los planes de tratamiento de riesgos consiste en determinar y detallar la manera en que tomarán las opciones seleccionadas, de modo que los involucrados entiendan y monitoreen el progreso del plan. De acuerdo con ISO 31000 el plan de tratamiento de riesgos permite reconocer claramente la disposición de la implementación de acciones, de tal forma que integre los procesos de gestión en la empresa, teniendo en cuenta las necesidades identificadas en atención a:

* Justificación para la elección de las opciones de tratamiento, incluyendo beneficios esperados.
* Quiénes son los responsables de aprobar e implementar el plan.
* Las acciones de tratamiento propuestas.
* Recursos requeridos, incluyendo los necesarios en caso de contingencia.
* Mediciones de rendimiento del plan.
* Limitaciones del plan.
* Acciones de monitoreo requeridas.
* Plazos esperados para que se completen las acciones.

Es importante reconocer la existencia de dos estrategias principales para el tratamiento de riesgos, estas son:

**Estrategias de evitación**

El objetivo es minimizar o reducir lo más posible la probabilidad de que el riesgo ocurra. El proceso se basa en:

* **Transferir**. Determina la eliminación del riesgo traspasándolo a un tercero, por ejemplo, el seguro contra terremotos de una casa, este riesgo se transfiere a una aseguradora.
* **Reducir**. El objetivo es minimizar la probabilidad de que ocurra un evento desafortunado, minimizando sus consecuencias o asegurando los objetivos propuestos. Contar con un sistema de gestión de riesgos adecuado a la organización permite reducir los riesgos de manera significativa.
* **Evitar**. Consiste en tomar la decisión acertada en el momento indicado, es decir, no ejecutar la actividad que trae consigo el riesgo, no poner en marcha el proyecto o contar con acciones alternativas de la actividad que ofrece los mismos resultados.
* **Diversificar**. Fraccionar el riesgo de un área en pequeñas secciones que incluyan otras áreas, con el fin de afectar todo el proyecto o la entidad en general (es mejor sacrificar un pequeño % de un área al 100 % del área).

**Estimación de minimización**

Reducen el impacto del riesgo en el proyecto. La minimización se presenta cuando falla la evitación y, por lo tanto, el riesgo se presenta. Se debe plantear un plan de contingencia para mitigar las consecuencias del riesgo, una vez este se haya creado.

* **Plan de contingencia.** Describe los procesos y los procedimientos que se deben implementar en una empresa cuando los riesgos dejan de ser probables y se convierten en un hecho. Por lo tanto, se asume que las acciones de monitoreo y control de los riesgos han fallado, y sus consecuencias son inevitables. Llegado a este punto, la única salida es activar el plan de minimización que incluye las etapas de coordinación en la administración de las crisis, y uso de los procedimientos que den la continuidad a las operaciones, y resolución de los incidentes para garantizar el reinicio de la operación normal de los procesos.

## 1.6 Normativa técnica

Son documentos donde se establece por consentimiento y con la aprobación de un ente reconocido algunas cláusulas o directrices mínimas que debe cumplir una empresa en la elaboración de un producto o servicio. Las normas son reglas que se aceptan de manera voluntaria por los interesados y a su vez reflejan la experiencia y el conocimiento de las personas, de acuerdo con su especialidad y las necesidades de las empresas.

Una de las normas más importante en la actualidad es la Norma ISO 31000, que ayuda a desarrollar y gestionar directrices en las empresas de cualquier sector económico, minimizando el impacto de los riesgos en todas sus áreas para mejorar los procesos y gestión de calidad.

A continuación, se presentan sus principales características:

* **Definición**

Norma internacional para la gestión de riesgos, que ofrece orientaciones y fundamentos para minimizar el impacto de los riesgos presentes en las organizaciones.

* **Origen**

Se publica en 2009 por la Organización Internacional de Normalización (ISO) en colaboración con la Comisión Electrotécnica Internacional (IEC).

* **Objetivos**
* Gestionar sistemas especializados para la normalización mundial.
* Apoyar a las empresas en el manejo de los riesgos de forma efectiva, recomendando el desarrollo, la implementación y la mejora continua de sus marcos de trabajo, con el propósito de integrar la cultura de gestión de riesgos en cada área de la organización.
* **Estructura**

Dada la diversidad y dificultad de los riesgos, la ISO 31000 no está enfocada en un sistema particular de gestión. Fue desarrollada como una guía de buenas prácticas para la implementación de acciones asociadas con la gestión de riesgos. Su diseño e implementación dependerá en gran medida de las necesidades de cada entidad, sus metas específicas, políticas, servicios, etc.

* Está compuesta de tres elementos fundamentales en la gestión de riesgos:
* Los principios para la gestión de riesgos.
* La estructura de soporte o marco de trabajo.
* El proceso de gestión de riesgos, este proceso consta de tres etapas: el
* establecimiento del contexto, la valoración de los riesgos y el tratamiento de los mismos.
* **Principios**
* **Crear y proteger el valor**. Contribuye a la consecución de objetivos así como la mejora de aspectos.
* **Estar integrada en los procesos de una organización**. No debe ser entendida como una actividad aislada, sino como parte de las actividades y procesos principales de una organización.
* **Formar parte de la toma de decisiones**. Ayuda a la toma de decisiones, evaluando la información sobre las distintas alternativas.
* **Tratar explícitamente la incertidumbre**. Aborda aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y cómo puede tratarse.
* **Ser sistemática, estructurada y adecuada**. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
* **Basarse en la mejor información disponible**. Los “inputs” del proceso de gestión del riesgo están basados en fuentes de información como la propia experiencia, la observación y la opinión de expertos.
* **Estar hecha a medida**. Alineada al contexto externo e interno de la organización y su perfil de riesgo.
* **Tener en cuenta factores humanos y culturales**. Reconoce la capacidad y la percepción de los empleados y personas interesadas.
* **Ser transparente e inclusiva**. La apropiada y oportuna participación de los grupos de interés (“stakeholders”) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanezca relevante y actualizada.
* **Ser dinámica, iterativa y sensible al cambio**. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa y de su entorno.
* **Facilitar la mejora continua de la organización**. Las organizaciones deberán desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

También están los sistemas de gestión de seguridad de la cadena de suministro ISO 28000 que permiten a las empresas tener la competencia de controlar las vulnerabilidades y las amenazas que lleguen afectar la seguridad. De la Norma ISO 2800 se destaca lo siguiente:

* Aporta un entorno de buenas prácticas para minimizar los riesgos de los responsables y los productos en la cadena de suministro.
* Gestiona y mitiga la seguridad en la logística, enfocándose a amenazas como el terrorismo, el fraude y la piratería.
* Permite a una empresa amortiguar las consecuencias de los incidentes de seguridad, centrándose en situaciones críticas para gestionar y garantizar los riesgos de seguridad de la cadena de suministro, incluyendo financiación, producción, gestión de la información, transporte, almacenamiento y/o depósito.

Como beneficios de la aplicación de esta norma en una compañía se puede destacar los siguientes:

* Permite identificar los riesgos y las amenazas que atentan contra la seguridad de la cadena de suministro e implementar controles para contrarrestar las amenazas.
* Reduce los niveles de inspección.
* Mejora la gestión del riesgo.
* Contribuye con la seguridad de los empleados.
* Mejora las relaciones y brinda mayor confianza con los organismos reguladores.
* Fortalece la continuidad del negocio.
* Contribuye a gestionar requisitos de otros sistemas de gestión.
* Permite mejorar continuamente la seguridad en la cadena de suministro.
* Generación de ventaja comercial y competitiva.

Las normas técnicas actúan como guías de normalización, unificando procesos y procedimientos que protegen los activos de las empresas, apoyándose en razones éticas, que promueven la calidad, la eficiencia y la seguridad. Su objetivo final es la estandarización para un correcto seguimiento, supervisión y desarrollo de los procesos, sin omitir que diferentes normas pueden integrarse y complementarse entre sí, razón por la cual las normas de gestión de riesgos trabajan en conjunto con las normas de gestión de calidad de la información.

# Gestión de la información

“La Política de Gobierno Digital es una política de Estado liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MinTIC que tiene como objetivo promover el uso y aprovechamiento de las TIC para fortalecer y garantizar un Estado y ciudadanos innovadores, competitivos y dinámicos, que otorguen valor público en un entorno de confianza digital.” (MinTIC, 2019, p. 11).

Esta política consiste en dos componentes que se desarrollan mediante tres habilitadores, todos en pro de lograr los cinco propósitos planteados para la implementación de esta política en las entidades públicas:

1. Servicios digitales de confianza y calidad.
2. Decisiones basadas en datos
3. Procesos internos, seguros y eficientes.
4. Empoderamiento de los ciudadanos a través del Estado abierto.
5. Territorios y ciudades inteligentes a través de las TIC.

En el siguiente esquema se presentan los elementos de la Política de Gobierno Digital:

* **Componentes**

Elementos constitutivos de la Política de Gobierno Digital que establece dos líneas de acción.

* **TIC para el Estado**

Busca mejorar el funcionamiento de las entidades públicas y su relación con otras entidades, por ejemplo, mejorar el funcionamiento del SENA y su interacción con entidades como el Ministerio de Educación o la Registraduría Nacional.

* **TIC para la sociedad**

Busca fortalecer la relación de los ciudadanos con el Estado promoviendo el uso de los datos públicos y participación del diseño de conjunto de servicios, políticas y soluciones a problemáticas de interés común, por ejemplo, que la ciudadanía participe activamente proponiendo necesidades de formación para servidores públicos y que en conjunto con el SENA se ofrezcan programas o acciones de capacitación para suplirlas.

* **Seguridad de la información**

El SENA implementa lineamientos de seguridad de la información en procesos, trámites y servicios, sistemas de información, infraestructura y en general en todos los activos de información, con el fin de preservar la confidencialidad, la integridad, la disponibilidad y la privacidad de los datos.

* **Arquitectura**

El SENA aplica el enfoque de arquitectura empresarial para la gestión de TI, lo que permite trazar el mapa de ruta respecto a los lineamientos y mejores prácticas para sus inversiones en tecnología.

* **Servicios ciudadanos digitales**

El SENA debe prestar servicios digitales a los ciudadanos como, por ejemplo, autenticación biométrica, autenticación con cédula digital, carpeta ciudadana, solicitud de certificaciones mediante medios electrónicos, entre otros.

* **Habilitadores Transversales**

Aspectos que articulados permiten el desarrollo de los componentes de la política.

Valor público

**Propósitos**

La Política de Gobierno Digital se orienta en la satisfacción de las necesidades y la solución de problemas del Estado y de los ciudadanos a través de la sincronía entre componentes y habilitadores, favoreciendo el logro de los siguientes cinco propósitos:

1. Que las entidades habiliten y mejoren la provisión de servicios digitales de confianza y calidad.
2. Que los procesos internos de las entidades públicas sean seguros y eficientes a través del fortalecimiento de las capacidades de gestión de las tecnologías de la información.
3. Que las entidades públicas tomen decisiones basadas en datos.
4. Que los ciudadanos se empoderen y participen de la consolidación de un Estado abierto.
5. Que se solucionen retos sociales mediante el desarrollo de territorios y ciudades inteligentes.

Así, el MinTIC dispone que, dentro de la sección de políticas TI, las entidades deben actuar junto a lineamientos, guías y estándares que les faciliten la gestión de sus recursos y proyectos, que conlleven a resultados más eficientes.

## 2.1 Protocolos de elaboración

La información es indispensable para abordar diferentes procesos administrativos, académicos, operativos, tecnológicos, etc. El tratamiento de la información en cualquier tipo de formato (digital, físico, magnético) es una de las actividades que realizan los sistemas de información que soportan los procesos. Del mismo modo, estos métodos incorporan los datos y los recursos físicos como el papel, o tecnológicos, así como los encargados de realizar estas actividades.

Al hablar de los activos que componen los sistemas de información se pueden reconocer los activos físicos (como los computadores) y los de almacenamiento (como USB, discos, cintas, etc.). No obstante, no es recomendable discriminar los demás activos, que aunque no son tangibles, sí son esenciales para las organizaciones como, por ejemplo, el conocimiento (“knowhow”) de los funcionarios, la reputación, el “software” o la propiedad intelectual.

Cuando se habla de los Sistemas de Gestión de Seguridad de la Información – SGSI se habla de reconocer la importancia del uso reflexivo de la tecnología y las comunicaciones, entendiendo que su uso irresponsable expone a diario a múltiples amenazas que ponen en riesgo la información y con ello, la operación de las entidades. Dichos riesgos provienen tanto del exterior como del interior. Para poder trabajar en un ambiente seguro es necesario identificar la información, determinar su valor e implementar mecanismos o controles en los procesos, las personas y la tecnología. Con el apoyo e implementación del Sistema de gestión de seguridad y privacidad de la información se puede identificar y gestionar los posibles riesgos que atenten contra la seguridad de la información de la empresa.

Para hablar del SGSI es importante entender los diferentes conceptos asociados y la diferencia entre seguridad de la información, seguridad informática y ciberseguridad, que se expone a continuación:

* **Seguridad informática**

Área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida en una computadora o circulante a través de las redes de las computadoras.

* **Ciberseguridad**

Reservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

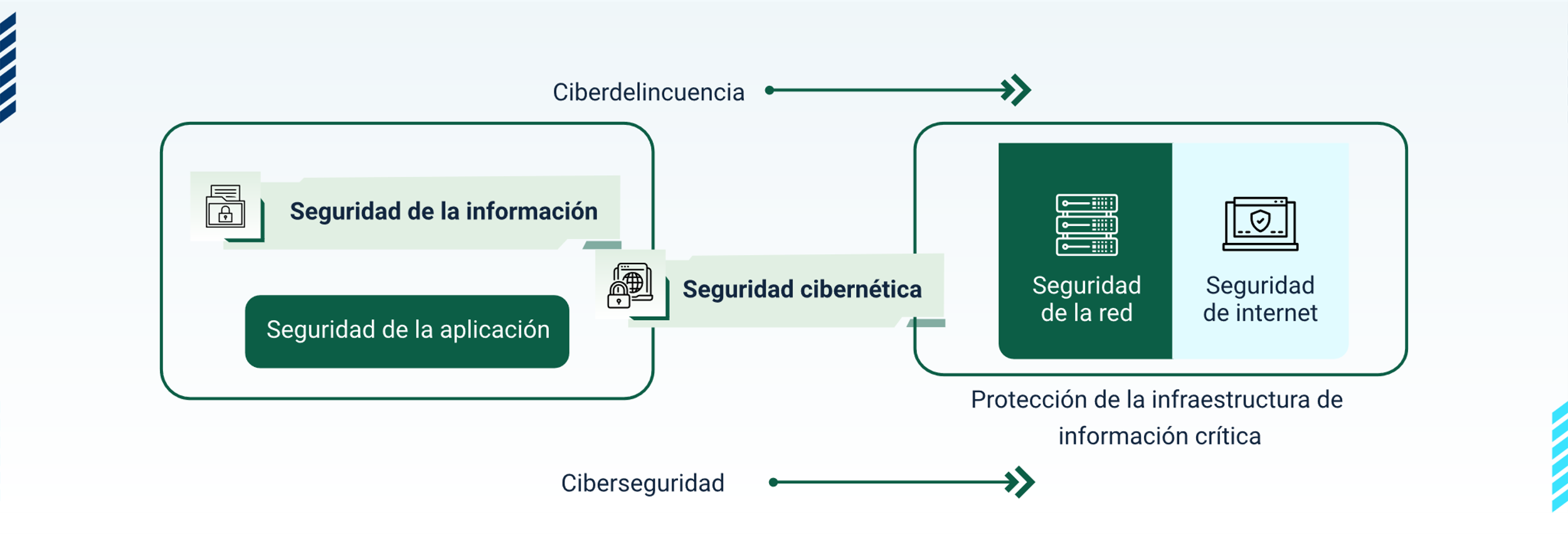
* **Seguridad de la información**

Reservación de la confidencialidad, la integridad y la disponibilidad de la información. También involucra otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad.

La **seguridad informática** permite resguardar toda la información, por lo que su alcance es mucho más amplio que la **ciberseguridad**; es decir, la SI protege la información de todos los posibles riesgos que puedan afectarla, bien sea por medio físico o digital. Por otro lado, la **ciberseguridad** está orientada a proteger la información digital que se procesa a través de redes, computadores, servidores, etc., por lo que se aproxima mucho a la **seguridad informática**, la cual se preocupa de la protección de la información en cualquier infraestructura computacional o medio informático interconectado o no.

La siguiente figura representa las relaciones entre ciberseguridad y otros dominios de seguridad:

1. Relaciones de ciberseguridad y otros dominios

****

**Relaciones de ciberseguridad y otros dominios**

**Ciberdelincuencia.**

Seguridad de la información.

Seguridad de la aplicación.

Seguridad cibernética.

Seguridad de la red.

Seguridad de internet.

**Ciberseguridad.**

Protección de la infraestructura de información crítica.

En conclusión, las bases de datos, los sistemas de información, los reportes, las facturas, los datos personales de contratistas, docentes, proveedores, etc., se deben gestionar de forma diferente, porque no todos tienen la misma relevancia. Por ello, lo más importante en el momento de proteger la información es clasificarla correctamente antes de tomar alguna acción.

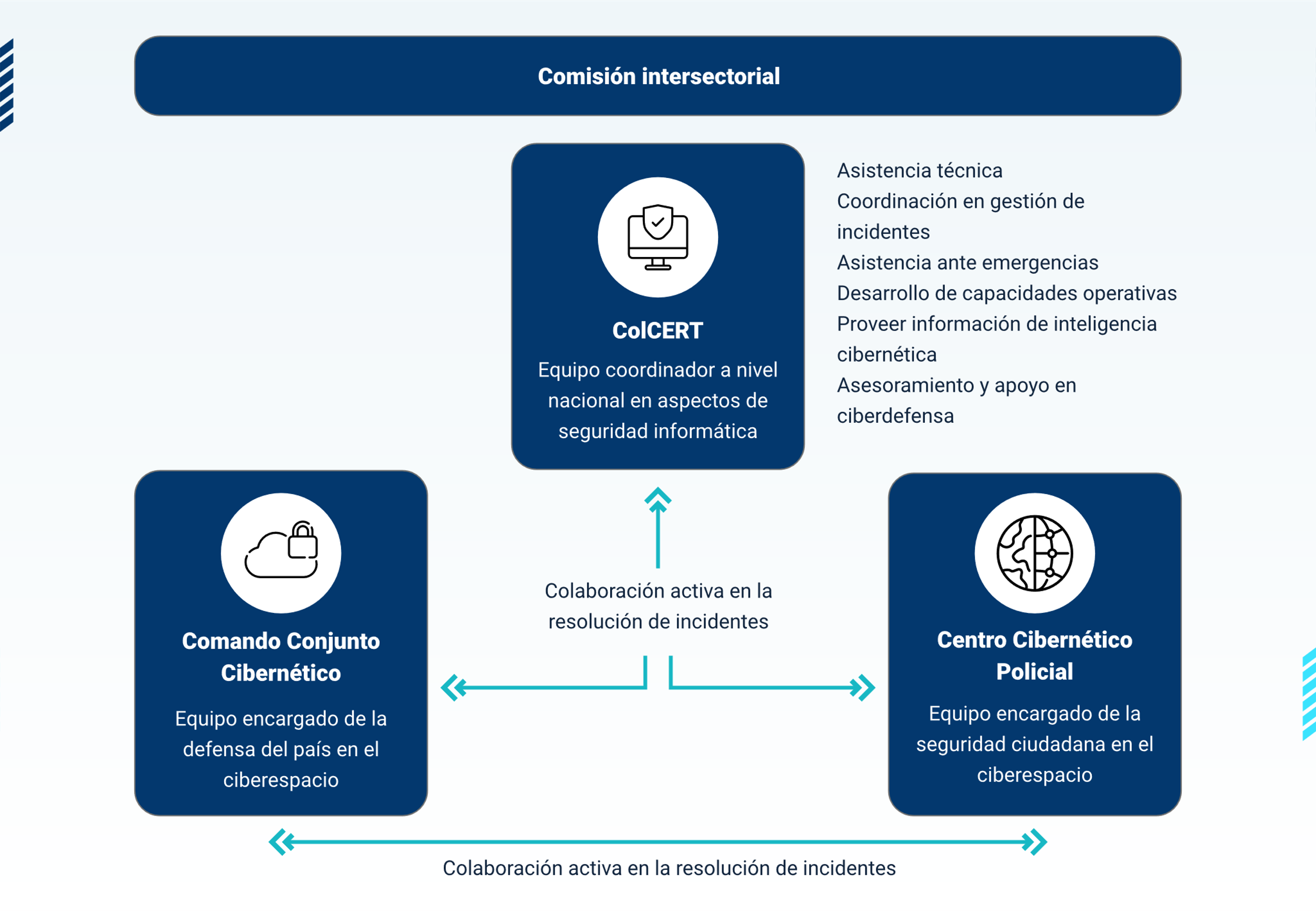
Por eso, la Ley de Protección de Datos Personales declara la protección como el derecho de toda persona a conocer, actualizar y rectificar la información recogida en bases de datos propensas a la manipulación y la gestión por entidades públicas o privadas. De acuerdo con esto, la información personal se encuentra clasificada así:

* **Pública**: dato público.
* **Clasificada**: dato semiprivado y privado.
* **Reservada**: dato sensible.

## 2.2 Normativa de protección de datos

En Colombia a partir de los Lineamientos de política para ciberseguridad y ciberdefensa establecidos en el CONPES 3701 del 14 de Julio de 2011 se crearon los equipos especializados en incidentes de seguridad que brindan servicios de respuesta a entidades del Estado, además de contribuir con el fortalecimiento de la seguridad y la generación de confianza ante la ciudadanía.

El siguiente esquema muestra el modelo de coordinación de la comisión intersectorial:

1. Modelo de coordinación comisión sectorial

Adaptado del Modelo de coordinación, Conpes (2011).

**Modelo de coordinación comisión sectorial**

Colaboración activa en la resolución de incidentes:

**ColCERT**

Equipo coordinador a nivel nacional en aspectos de seguridad informática.

* Asistencia técnica.
* Coordinación en gestión de incidentes.
* Asistencia ante emergencias.
* Desarrollo de capacidades operativas.
* Proveer información de inteligencia cibernética.
* Asesoramiento y apoyo en ciberdefensa.

**Comando conjunto cibernético**

Equipo encargado de la defensa del país en el ciberespacio.

**Centro cibernético policial**

Equipo encargado de la seguridad de la ciudadanía en el ciberespacio.

Colaboración activa en la resolución de incidentes.

Con el aumento del uso de las tecnologías y los incidentes generados a partir de estas, el Gobierno Nacional el 6 de agosto de 2018 inauguró el CSIRT de gobierno, un equipo que presta el servicio de prevención y respuesta a los incidentes de seguridad informática que afectan a las entidades públicas del país.

La Ley 1712 de 2014 creó la **Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional**, que obliga a publicar en las páginas web tres instrumentos de gestión con el fin garantizar la transparencia y el acceso a la información pública por parte de todos los ciudadanos:

* Registro de activos de la información.
* Índice de información clasificada y reservada.
* Esquema de publicación.

La NTC-ISO/IEC 27001 es una norma certificable, creada por la ISO con el objetivo de proporcionar una metodología universal para implementar, administrar y mantener la seguridad de la información. De acuerdo con esta norma, el SGSI está conformado por los elementos dispuestos en la siguiente gráfica que representa de modo piramidal las diferentes fases que acompañan los principios del SGSI:

1. Principios

Figura 4. Figura que contiene una pirámide de los principios del SGSI, los cuales son:
Lineamientos.
Procesos.
Procedimientos.
Estándares.
Arquitectura/Servicios.

**Principios**

Procesos.

Procedimientos,

Estándares.

Arquitectura/servicios.

Integridad.

**Disponibilidad.**

**Confidencialidad – privacidad.**

La protección de la información se realiza manteniendo los principios (confidencialidad, integridad y disponibilidad) donde esté, incluye los dispositivos que la almacenan, procesan y transmiten, y todos los recursos que intervienen en su ciclo de vida, las personas, los procesos y la tecnología que se utilicen; todo esto mediante el uso de políticas, procedimientos, sensibilización y tecnologías.

Proteger la información de amenazas que lleguen a afectar la integridad, la confidencialidad y la disponibilidad es lo que se denomina Sistema de información - SI. Conocer los principios de seguridad que se deben proteger permite identificar de manera más fácil las medidas de protección que deben ser aplicadas para evitar su pérdida o alteración, a continuación, se exponen dichos principios:

* **Disponibilidad**

Propiedad mediante la cual la información es accesible y utilizable por solicitud de una entidad autorizada (ISO IEC-27001 de 2009), por ejemplo, una falla de disponibilidad se presenta cuando no es posible acceder a un sistema, archivo o documento debido a un error de configuración, un virus o simplemente porque se perdió.

* **Confidencialidad**

Propiedad de protección de la exactitud y completitud de la información, por ejemplo, una falla de integridad ocurre cuando la información ha sido alterada sin autorización o fue borrada, accidentalmente o no. Otros ejemplos de fallos de integridad son el borrado parcial, accidental o no, de bases de datos, archivos o programas.

* **Seguridad de la información**

Propiedad mediante la cual la información no se hace disponible o revelada a individuos, entidades o procesos no autorizados, es decir, la información confidencial es aquella que una vez identificada, se protege del acceso de personas no autorizadas.

A continuación, se presentan los elementos de la Ley de Protección de Datos Personales y la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional:

**Ley de protección de datos personales Ley 1581 de 2012**

Permite saber cómo identificar un dato personal de acuerdo con la tipología que define la ley y así realizar la correcta clasificación de la información. Clasificados así:

* **Dato personal**. Toda la información de una persona que permite su identificación (documento de identificación personal, fecha de nacimiento, edad, sexo, estado civil, trayectoria laboral, entre otros).
* **Dato público**. Determinado así por la ley o la Constitución Política de Colombia, también aquellos que no sean semiprivados o privados.
* **Dato semiprivado.** No tiene naturaleza íntima, reservada, ni pública. Su conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas.
* **Dato privado**. De naturaleza íntima o reservada, solo es relevante para el titular de la información.
* **Dato sensible**. Afecta la intimidad del titular. Su uso indebido puede generar discriminación (origen racial o étnico, orientación política, convicciones filosóficas o religiosas, pertenencia a sindicatos u organizaciones sociales o de derechos humanos, datos de salud, vida sexual y biométricos).

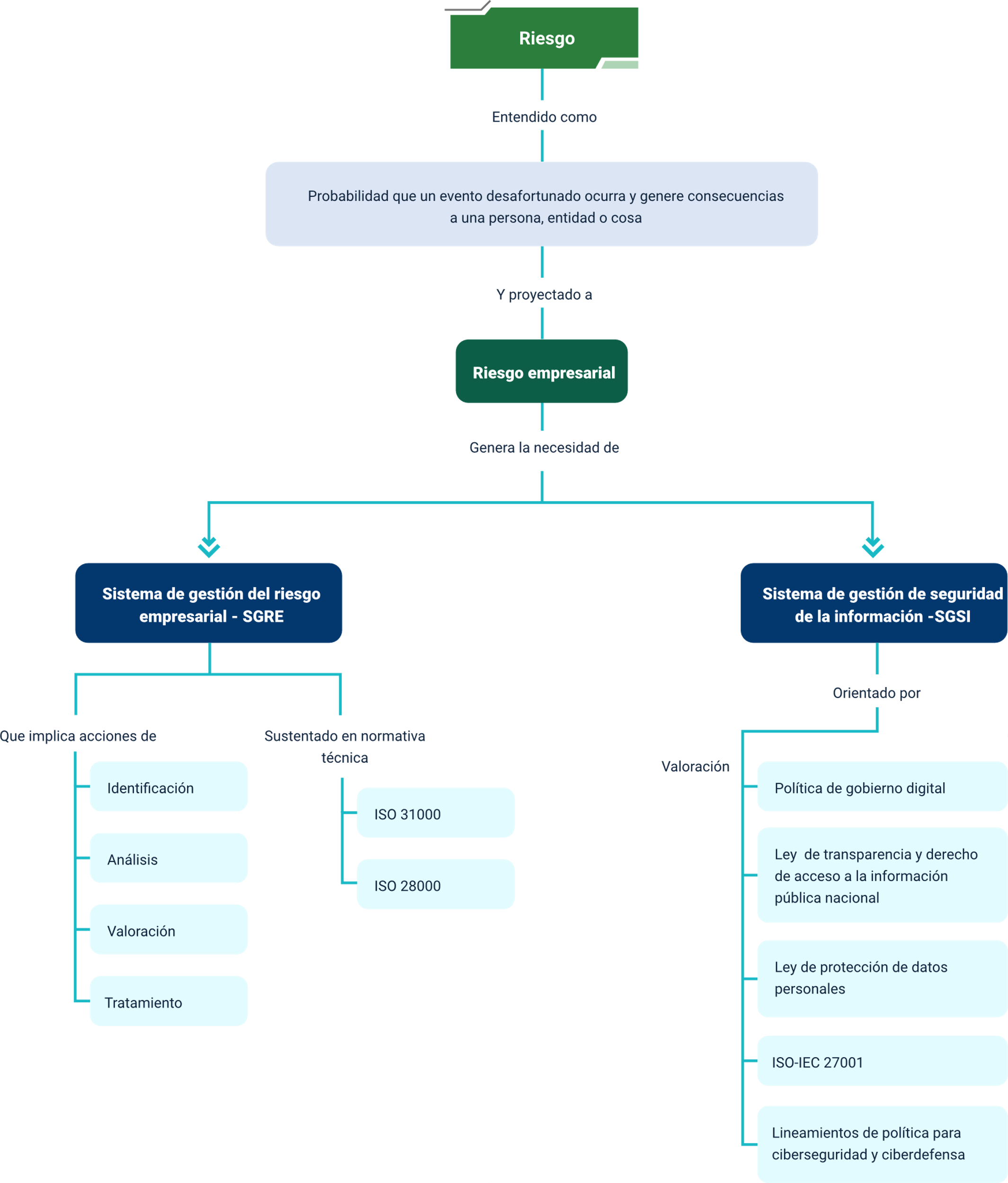
**Ley de transparencia y del derecho de acceso a la información pública nacional Ley 1712 de 2014**

Clasifica la información en tres categorías:

* **Pública**. Aquella que un sujeto obligado genere, obtenga, adquiera o controle.
* **Pública clasificada**. Aquella que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado siempre que se trate de las circunstancias legítimas y necesarias y, los derechos particulares o privados consagrados en la ley.
* **Pública reservada**. Aquella que estando en poder de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de los requisitos consagrados en la ley.

Síntesis

El siguiente esquema presenta el resumen de las temáticas desarrolladas en el componente formativo, destacando la importancia de los sistemas de gestión del riesgo y la seguridad de la información para el logro de los objetivos empresariales y contribución al proceso de mejora continua de las organizaciones:



Material complementario

| Tema | Referencia APA del Material | Tipo de material | Enlace del Recurso o  Archivo del documento material |
| --- | --- | --- | --- |
| Evaluación del riesgo | Ecuador. Secretaría de Gestión de Riesgos. (2012). Ecuador: referencias básicas para la gestión de riesgos 2013-2014. Secretaría de Gestión de Riesgos. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_elibroELB30908&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| Normativa técnica | Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2016). Gestión del riesgo: orientación para la implementación de la NTC-ISO 31000. Icontec | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000012244&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| Normativa de  protección de datos | Chaparro, M. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. Inventum, 9(17), p. 32-37. | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_doaj_primary_oai_doaj_org_article_d369f2b22f8f479ca3bbdf0c2f4ad238&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC> |

Glosario

**Datos:** cualquier objeto que pueda entregar información o significado para el lector. El dato puede ser manipulable en forma manuscrita o por medio de un computador. Puede ser un carácter capturado desde un teclado, extraído de algún espacio de memoria en el disco, almacenado en la memoria central, etc.

**Gestión de riesgo:** proceso que afecta a todos los órganos directivos y laborales de la organización (junta directiva, administrativos y empleados).

**Mapa de riesgos**: identifica de forma gráfica los riesgos a los que se expone una empresa, teniendo en cuenta la probabilidad y el impacto que pueden causar.

**Riesgo:** probabilidad de que un evento desafortunado ocurra y genere consecuencias a una persona, entidad o cosa.

**Seguridad de la información:** se encarga de proteger los datos contra robo de información, acceso no autorizado, obstaculización al sistema informático, manipulación y/o eliminación de los datos.

Referencias bibliográficas

Comunidad de Madrid. (s.f.) Tratamiento del riesgo. Comunidad de Madrid. <http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo%28AR%29_es.pdf>

Consejo Nacional de Política Económica y Social. (2011). Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa. Consejo Nacional de Política Económica y Social. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Cristo, N. (2019). 6 reglas para gestionar riesgos en las empresas. Grupo Bancolombia. <https://www.bancolombia.com/empresas/capital-inteligente/actualidad-economica-sectorial/6-reglas-gestionar-riesgos-empresariales>

Hopkin, P. (2010). “Fundamentals of risk management: understanding, evaluating, and implementing effective risk management”. Kogan Page Limited.

Londoño, I. (2020). Mapa de calor: una herramienta para optimizar la gestión de riesgos. Pirani. <https://www.piranirisk.com/es/blog/mapa-de-calor-una-herramienta-para-optimizar-la-gestion-de-riesgos>

Martínez, J. (2011). Riesgo e incertidumbre. ScalabBle. <http://www.scalabble.com/2011/03/riesgo-e-incertidumbre/index.html>

Ministerio de Tecnologías de la Información y las Comunicaciones-MinTIC. (2019). Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital. MinTIC. <https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Milady Tatiana Villamil Castellanos | Líder Ecosistema de Recursos Educativos Digitales | Dirección General |
| Liliana Victoria Morales Gualdrón | Responsable Líder Línea de Producción Tolima | Regional Tolima – Centro de Comercio y Servicios |
| Abel Fernando Becerra Carrillo | Experto Temático | Regional Norte de Santander - Centro de la industria, la empresa y los servicios |
| Jeimy Lorena Romero Perilla | Diseñadora Instruccional | Regional Norte de Santander - Centro de la industria, la empresa y los servicios |
| Silvia Milena Sequeda Cárdenas | Asesora Metodológica | Regional Distrito Capital - Centro de Diseño y Metrología |
| Sandra Patricia Hoyos Sepúlveda | Correctora de Estilo | Regional Distrito Capital - Centro de Diseño y Metrología |
| Andrés Felipe Velandia Espitia | Evaluador Instruccional | Regional Tolima – Centro de Comercio y Servicios |
| Lina Marcela Pérez Manchego | Diseñadora de Contenidos Digitales | Regional Tolima – Centro de Comercio y Servicios |
| Sebastián Trujillo Afanador | Desarrollador FullStack | Regional Tolima – Centro de Comercio y Servicios |
| Norma Constanza Morales Cruz | Evaluadora de Contenidos Inclusivos y Accesibles | Regional Tolima – Centro de Comercio y Servicios |
| Javier Mauricio Oviedo | Validador y Vinculador de Recursos Educativos Digitales LMS | Regional Tolima – Centro de Comercio y Servicios |