Libertad y Orden

Gobernación de Nariño

Secretaría
TIC, Innovación
y Gobierno Abierto

GOBERNACION DE NARIÑO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ENERO 2021

Calle 19 No 23-78 / Codigo Postal: 520003 | 123
contactenos@narino.gov.co - www.narino.gov.co
Pasto-Nariño-Colombia

INTROCUCCION

La Seguridad de la Información en las entidades tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta.

La Gobernación de Nariño enmarcada en el proceso anteriormente descrito y con el fin de dar cumplimiento a la política de seguridad de la información, debe aplicar el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación, para el correcto desempeño dentro de la política pública y su relación con el ciudadano

Los principios de protección de la información se enmarcan en:

• Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

• Integridad: Propiedad que la información se mantenga exacta y completa.

• Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVO GENERAL

Brindar a la Gobernación de Nariño una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, para los procesos y procedimientos incluidos en el alcance del Sistema de Seguridad de la Información y MIPG alineadas con la Norma NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio. Utilizando los métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

El Plan de Tratamiento para los riesgos de seguridad y privacidad de la información permita disminuir la probabilidad y el impacto de riesgos de seguridad y privacidad de la información que puedan afectar a la Gobernación de Nariño. para proporcionar una seguridad e integridad razonable que genere una base confiable para la toma de decisiones y la planificación institucional.

OBJETIVOS ESPECÍFICOS

1. Identificar y sensibilizar a la entidad para la construcción de acciones que conlleven al fortalecimiento de la Entidad frente a la seguridad y privacidad de la información.

2. Revisar, ajustar y/o validar la Política de la Entidad de Gestión de Riesgos de seguridad y privacidad de la información.

3. Generar un panorama de la Entidad para la construcción de planes políticas y controles para un adecuado tratamiento de riesgo de seguridad y privacidad de la información.

4. Definir y desarrollar estrategias para la elaboración del plan de tratamiento de riesgos de seguridad y privacidad de la información con priorización de aspectos críticos identificados, validando los recursos con los que se cuentan actualmente en la Gobernación de Nariño.

5. Conocer y explorar las metodologías del DAPF[1] e ISO[2] respectivamente en seguridad y riesgo de la información.

[1] DAPF es el Departamento Administrativo de la Función Pública de Colombia ISO

[2] ISO es International Organization for, que en español traduce, Organización Internacional de Normalización

6. Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas

7. Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas

8. Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.

ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, deberá será aplicada sobre cualquier proceso de la Gobernación de Nariño, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

NORMATIVIDAD

La normatividad en el cual se enmarca el Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se encuentra dentro del marco de la legislación alusiva al Sistema de gestión pública del Estado Colombiano, especialmente de la Política de Gobierno Digital y articulada con la reglamentación y lineamientos producidos por la legislación Colombiana, Decreto reglamentarios, el Departamento Administrativo de la Función Pública y el Ministerio de las TIC, como, Habeas DATA, Propiedad Intelectual, Seguridad Digital, Servicios Ciudadanos Digitales, Participación Democrática, Transparencia, Acceso a la Información Pública y Anticorrupción, entre otros.

RESPONSABILIDAD Y AUTORIDAD El desarrollo y actualización del plan está bajo la autoridad de la Dirección o área responsable del proceso de Gestión Tecnológica, o quién haga sus veces dentro del contexto de las Tecnologías de la Información y las Comunicaciones que establezca oficialmente la Gobernación de Nariño para tal finalidad, o quién lo reemplace o sustituya. Actualmente es la Secretaria TIC, Innovación y Gobierno Abierto, quien podrá editar el contenido de cada una de las secciones que lo conforman, previa aplicación del comité MIPG.

TÉRMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

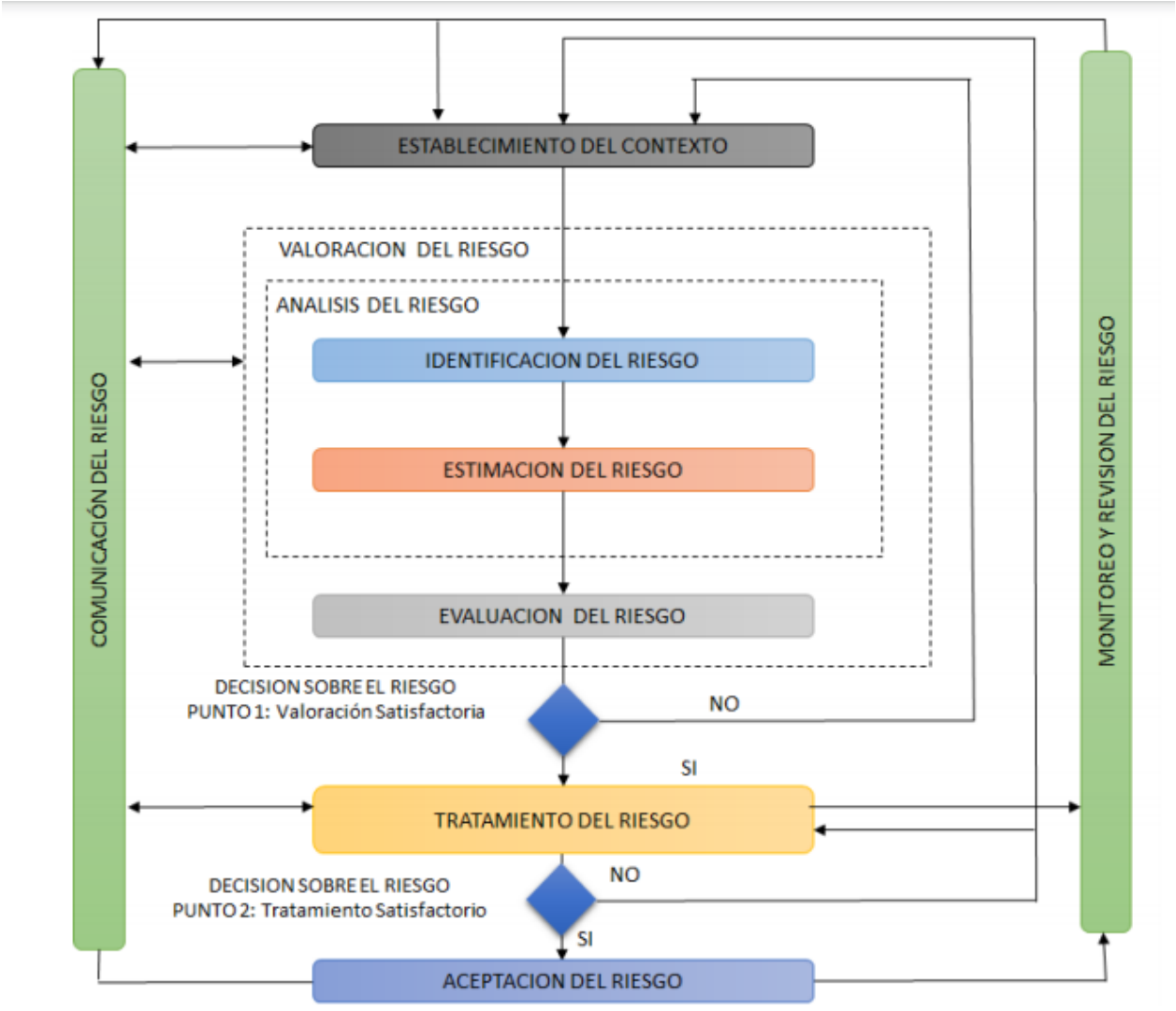
Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO/IEC 27005, para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



1. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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

Criterios de evaluación del riesgo de seguridad de la información:

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

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

Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Agencia, causados por un evento de seguridad de la información, considerando aspectos tales como:

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

Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la Gobernación de Nariño y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del documento

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas

- Factores sociales y humanitarios

2. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Durante esta etapa se tiene en cuenta los activos de la información identificados, ya que son la base para la valoración de los riesgos de seguridad de la información. Se deberán identificar los riesgos, describir cuantitativamente o cualitativamente y priorizar frente a los criterios de evaluación determinados en la fase anterior

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

2.1 Identificación del riesgo. Se deberán identificar los activos de información por proceso, teniendo en cuenta su clasificación:

2.1.1. Primarios:

2.1.1.1. Procesos o subprocesos y actividades del Negocio: procesos cuya modificación y/o pérdida hacen imposible o afectar de manera muy significativa la misión de la Entidad, procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

2.1.1.2. Información: información vital para la ejecución de la misión de la Entidad, información estratégica que se requiere para alcanzar los objetivos estratégicos de la Entidad, información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición.

2.1.1.3. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

2.1.2. De Soporte

2.1.2.1. Hardware: Elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

2.1.2.2. Software: Programas que contribuyen al funcionamiento de la Entidad (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

2.1.2.3. Redes: Dispositivos de telecomunicaciones tales como conmutadores, cableado, puntos de acceso, etc.

2.1.2.4. Personal: Grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

2.1.2.5. Sitio: Lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

2.1.2.6. Estructura organizativa: responsables, áreas, contratistas, etc.

Una vez clasificados los activos de la información se deben determinar los mecanismos a utilizar para identificar y valorar las **amenazas** que pueden causar daños en la información, los procesos y los soportes, así mismo los cronogramas de aplicación. Una vez identificadas

las amenazas se identifican las vulnerabilidades y las consecuencias es decir cómo se afecta la confidencialidad, integridad y disponibilidad de los activos de información

2.2. Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para la estimación es necesario contar con el personal que tenga conocimiento de los procesos ya que se debe tener en cuenta pérdidas financieras, costos de reparación o sustitución, interrupción del servicio, infracciones legales, competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán definir los mecanismos para estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información, se deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

PROBABILIDAD	1 - Insignificante	2 - Menor	3 - Moderado	4 - Mayor	5 - Catastrófico
1 - Raro	Bajo	Bajo	Moderado	Alto	Alto
2 - Improbable	Bajo	Bajo	Moderado	Alto	Extremo
3 - Posible	Bajo	Moderado	Alto	Extremo	Extremo
4 - Probable	Moderado	Alto	Alto	Extremo	Extremo
5 - Casi Seguro	Alto	Alto	Extremo	Extremo	Extremo

- Impacto: Hace referencia a las consecuencias que puede ocasionar a la Gobernación de Nariño la materialización del riesgo; se refiere a la magnitud de sus efectos.

DESCRIPTOR	POSIBLES EFECTOS			
	PERSONAS	ECONÓMICO	IMAGEN	AMBIENTAL

5 - Catastrófico	* Indisponibilidad de más del 50% de personal clave en procesos críticos * Lesiones Fatales	Pérdidas en ventas Demandas contractuales y multas Pérdidas en la competitividad Alquiler temporal de equipos, instalaciones y personal Traslado de equipos, suministros y personal Reconstrucción de los sistemas	Imagen Pública Negativa Pérdida de confianza de los inversionitas Moral de los empleados Sanciones * Pérdida grave del apoyo o credibilidad de los grupos de interés que se traduzca en una intervención o cambio de regulación	* Daño ambiental grave recuperable a largo plazo o que puede afectar áreas sensibles o comunidades
4 - Mayor	* Indisponibilidad de entre 20% al 50% de personal clave en procesos críticos * Lesiones con incapacidad parcial o total permanente	Nivel de perdidas no aceptables	* Disminución sensible del apoyo o credibilidad de algunos de los grupos de interés que se traduzca en regulaciones que sean desfavorables	* Daño ambiental significativo recuperable a mediano plazo o con impacto directo en la actividad económica de terceros
3 - Moderado	* Indisponibilidad de menos del 20% de personal clave en procesos críticos * Indisponibilidad de personal clave en procesos no críticos * Lesiones con incapacidad total temporal	• Interrupción de las operaciones de la Entidad entre uno (1) y dos (2) días. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.	* Inquietudes o cuestionamientos por parte de los grupos de interés que se traduzcan en sanciones económicas	* Daño ambiental importante recuperable a corto plazo
2 - Menor	* Indisponibilidad de personal no clave en procesos críticos * Lesiones con incapacidad parcial temporal (trabajo restringido)	• Interrupción de las operaciones de la Entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	* Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. *Concepto desfavorable en un segmento de clientes o en un cliente importante * Inquietudes o cuestionamientos a nivel general	* Daño ambiental leve o transitorio recuperable en el corto plazo
1 - Insignificante	* Indisponibilidad de personal no clave en procesos no críticos * Lesiones sin incapacidad pero que requieren atención de primeros auxilios o tratamiento médico	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas.	* No se afecta la imagen institucional de forma significativa *Difusión interna a nivel de proceso o equipo de trabajo * Inquietudes o cuestionamientos	Contaminación puntual sin consecuencias para el ambiente

2.3. Determinación del riesgos

La valoración de los riesgos de Información se hace de manera cualitativa, generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la Matriz IP, con la cual se presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

	MEDICION DE LA PROPABILIDAD E IMPACTO (CONSECUENCIAS)				
PROBABILIDAD	**1 - Insignificante**	**2 - Menor**	**3 - Moderado**	**4 - Mayor**	**5 - Catastrófico**
1 - Raro	B	B	M	A	A
2 - Improbable	B	B	M	A	E
3 - Posible	B	M	A	E	E
4 - Probable	M	A	A	E	E
5 - Casi Seguro	A	A	E	E	E

ZONA DE RIESGO

B	Zona de Riesgo Baja	Asumir el Riesgo
M	Zona de Riesgo Moderado	Asumir el Riesgo, Reducir el Riesgo
A	Zona de Riesgo Alta	Reducir el Riesgo, Evitar, Compartir o Transferir
E	Zona de Riesgo Extrema	Reducir el Riesgo, Evitar, Compartir o Transferir

2.4. Evaluación del riesgo

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, con ello es necesario definir los mecanismos de evaluación que permitirán compararlos frente a los criterios básicos del contexto, con el fin de tomar decisiones adecuadas basados en reducir los impactos en riesgos de seguridad de la información.

La valoración de los riesgos se puede consultar en el documento IDENTIFICACION Y VALORACION DE RIESGOS, VULNERABILIDADES Y AMENAZAS GOBERNACION DE NARIÑO

3. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se deberá elegir los mecanismos y/o estrategia de tratamiento del riesgo según su valoración y de los criterios establecidos en el contexto de gestión de riesgos, según la

matriz de riesgos que contiene la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, obtenida en las etapas anteriores.

Se deberá seleccionar la opción de tratamiento por cada uno de los riesgos identificados, de acuerdo con el nivel evaluación de los riesgos, así como tener en cuenta como factor relevante el costo/beneficio del tratamiento para la decisión.

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

Como resultado de esta fase se seleccionan las opciones de tratamiento para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas, lo anterior deriva en el plan de tratamiento de riesgos, en el cual se identifican los controles aplicables considerando las posibles limitantes para su implementación tales como restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal, entre otros

La Secretaria Tic, Innovación y Gobierno Abierto, con su equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

- La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados,
- Documento de declaración de aplicabilidad
- Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de los mismos y la prioridad de implementación de cada proyecto. Estos planes de proyectos de seguridad de la información son identificados y definidos en conjunto entre La Secretaria Tic, Innovación y Gobierno Abierto y los responsables de los procesos.

4. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que los riesgos son dinámicos y pueden cambiar de forma sin ser previsto es necesario definir mecanismos que permitan hacer una supervisión continua que detecte: nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información.

En este sentido se deben establecer instrumentos para realizar la revisión del valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

También se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información, con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.