Plan de Tratamiento de Riesgos Seguridad y Privacidad de la Información

2024

Instituto de Valorización de Manizales

INVAMA

Manizales, Enero 2024

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

CONTENIDO

INTRODUCCIÓN 6
1. OBJETIVO 7
1.1. OBJETIVOS ESPECIFICOS 7
2. ALCANCE 8
3. TÉRMINOS Y DEFINICIONES 9
4. MARCO NORMATIVO 13
5. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 16
6. METODOLOGÍA 18
6.1 Establecimiento del Contexto 20
6.2 Análisis de riesgos 22
6.3 Valoración del Riesgo 34
6.4. Tratamiento de Riesgos 36
6.5. Comunicación de Riesgos 37
6.6. Monitoreo - Información de Riesgos y revisión 38
6.7. Declaración de Aplicabilidad (SOA). 38
7. MAPA DE RUTA 40

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

INDICE DE FIGURAS

Figura 1. Interacción entre el MSPI y el MGRSD 19

Figura 2. Proceso de Gestión de Riesgos de Seguridad de la Información 20

Figura 3. Establecimiento del Contexto Interno 21

Figura 4. Establecimiento del Contexto Externo..... 22

Figura 5. Criterios de Probabilidad..... 32

Figura 6. Criterios de impacto 33

Figura 7. Matriz de Calificación, Evaluación y Respuesta a los Riesgos 34

Figura 8. Rango de Calificación de los Controles..... 36

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

INDICE DE TABLAS

Tabla 1. Catálogo de Amenazas Comunes establecidos en la ISO/IEC 27005 23

Tabla 2. Vulnerabilidades por Tipo de Activos y Amenazas 26

Tabla 3. Consecuencias por Tipo de Riesgo 30

Tabla 4. Atributos para Calificación del Control 35

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer la disponibilidad, integridad y confiabilidad de la información.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad de la información como habilitador de la política de Gobierno Digital adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior del Instituto de Valorización de Manizales - INVAMA, aprobado mediante acto administrativo de la sesión del comité de gestión y desempeño institucional.

1. OBJETIVO

Realizar la identificación, análisis, valoración y tratamiento de los riesgos y controles de seguridad de la información a los procesos del Instituto de Valorización de Manizales – INVAMA.

1.1. OBJETIVOS ESPECIFICOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios a los que el Instituto de Valorización de Manizales pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las Normas Técnicas Colombianas.

- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios del INVAMA.

2. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Adicionalmente dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Instituto de Valorización de Manizales – INVAMA.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Mayor y Catastrófico acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

3. TÉRMINOS Y DEFINICIONES

Con el propósito de facilitar la comprensión de este documento se describen las siguientes definiciones:

- **Activo de Información:** Todo lo que tiene valor para el INVAMA y que contiene, genera, procesa, almacena y le da un tratamiento a la información o se relaciona con la misma. Existen diferentes tipos de activos como: Información (bases de datos, bases de conocimiento), tecnológicos o digitales (hardware y software), infraestructura física (instalaciones, oficinas), organizacionales (procesos, metodologías, servicios) y el recurso humano (Empleados de Planta, Contratistas, proveedores, Terceros).

- **Ciberseguridad**: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

- **Confidencialidad:** Atributo de la información que determina quién está autorizado a acceder a ella y previene su divulgación no autorizada dentro del INVAMA.

- **Contraseña Fuerte:** Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.

- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla en caso de que ocurra un fallo que afecte a esta y pueda estar disponible.

- **Custodio de activo de información**: Parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad.

- **Disponibilidad:** Atributo de la información que determina para quién está disponible y los permisos de su uso dentro de las gestiones que adelante en el INVAMA.

- **Gestión de claves:** son controles que se realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** Son las acciones de control para garantizar la seguridad de los activos de información y su apropiada gestión, implementando las acciones para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información en el INVAMA.

- **Gestión de riesgos:** Son las acciones que realiza el INVAMA para la identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

- **Impacto**: El costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - p.ej., pérdida de reputación, implicaciones legales, etc. Consecuencia que sobre un activo tiene la materialización de una amenaza.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete al INVAMA.

- **Información:** Es un activo de valor que hace parte de la Agencia Nacional Digital, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la Entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

- **Integridad:** Atributo de la información que protege los activos de información sobre posibles alteraciones, modificaciones no autorizadas formalmente por el INVAMA.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, intangibles, etc.) dentro del

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

alcance del SGSI, que tengan valor para el INVAMA y necesiten por tanto ser protegidos de potenciales riesgos.

- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Principios de Seguridad de la Información**: son características propias de la protección de la información: la Confidencialidad, Integridad y Disponibilidad.

- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** Es la probabilidad de que una amenaza o vulnerabilidad pueda ocasionar la pérdida y/o alteración de la información del INVAMA

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la Accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información

- **Vulnerabilidad:** Es la debilidad o fallo del sistema que pone en riesgo la confidencialidad, integridad y disponibilidad de la información del INVAMA

- **Norma:** Principio que se dispone de carácter general, donde se establecen las obligaciones, restricciones y orientaciones para el acceso y uso de los activos de información.

- **Política:** Declaración de alto nivel que describe la posición del INVAMA sobre un tema específico.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

- **Procedimiento:** Documento que define los pasos a seguir y que deben ser implementados en una situación dada.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

4. MARCO NORMATIVO

- **Guías de implementación del MSPI – MinTIC.** 1. articles-5482 Modelo de Seguridad Privacidad.

- **ISO 27001:2013.** Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

- **ISO 27002:2015.** Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

- **ISO 27005:2009.** Gestión de Riesgos de Seguridad de la Información.

- **ISO 27017:2015.** Código de buenas prácticas de seguridad servicios en la nube.

- **ISO 27018:2014.** Código de práctica protección de información personal en nubes públicas.

- **ISO 27035:2012.** Buenas prácticas de gestión de incidentes de seguridad de información.

- **ISO 22301:2012.** Requisitos Sistema de Gestión de la Continuidad del Negocio.

- **ISO 31000:2018.** Gestión del Riesgo – Directrices

- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas**. Guía de gestión de riesgos del DAFP.

- **Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)**

- **NIST framework Ciberseguridad**, es el marco que permite a las organizaciones comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

- **Ley 1581 de 2012.** Protección datos personales. Circular 005 de 2017 SIC (Países Autorizados).

- **Ley 1712 de 2014.** Transparencia y del Derecho de Acceso a la Información Pública.

- **Ley 1273 de 2009.** Delitos informáticos

- **Ley 597 de 1999.** Acceso y uso mensajes de datos, comercio electrónico y firmas digitales.

- **Ley 23 de 1982**. Derechos de autor.

- **Ley 594 de 2000**. Ley general de archivo.

- **Decreto 2578 de 2012.** Reglamenta el Sistema Nacional de Archivos.

- **CONPES 3854 de 2016** – Política de Seguridad Digital del Estado Colombiano.

- **Decreto 1008 de 2018**. Política de Gobierno Digital.

- **Decreto 612 de 2018.** Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- **Decreto 620 de 2020**. Lineamientos generales en el uso y operación de los Servicios Ciudadanos Digitales.

- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital

- **Resolución 500 de 2021.** Lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

- **Decreto 338 de 2022.** Lineamientos generales para fortalecer la gobernanza de la seguridad digital

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

5. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Instituto de Valorización de Manizales – INVAMA, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos, en las actividades desarrolladas por la Entidad

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos y establecen las guías de acción necesarias a todos los colaboradores del INVAMA.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- Asumir el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Gestión y Desempeño Institucional (Comité de Seguridad de la Información) indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves.

- Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. Normalmente

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

se utiliza cuando la evaluación del riesgo es muy alta, o los costos para implementar los controles exceden los beneficios de su implementación.

- Transferir el riesgo: Alternativa más económica en caso de que sea muy costoso o difícil reducir o controlar un riesgo. Sin embargo, al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6. METODOLOGÍA

La metodología de gestión de identificación, evaluación y gestión de riesgos de seguridad y privacidad de la información del INVAMA, se basa en la NTC-ISO 27005:2011, la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública - DAFP y la Guía de la Secretaria de Transparencia de la Presidencia de la República, denominada Guía para la Gestión de Riesgo de Corrupción y Modelo de Gestión de Riesgos de Seguridad Digital – MGRSD, la Guía 7 de gestión de riesgos emitida por el MinTIC y la guía para la administración de riesgos y el diseño de controles en entidades públicas, las cuales están alineadas con la NTC – ISO/IEC 27005. Su propósito es la identificación, estimación y evaluación de los riesgos de la Entidad para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos.

El Modelo de Seguridad y Privacidad de la Información integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el MSPI.

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

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

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

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

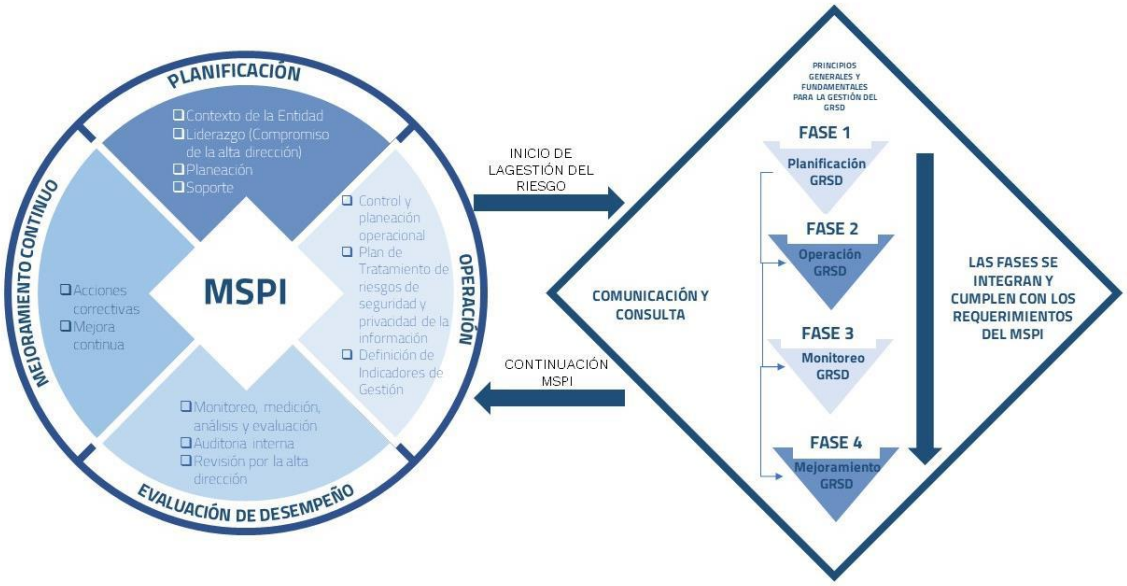

Figura 1. Interacción entre el MSPI y el MGRSD

Fuente: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Esta metodología se desarrolla en 8 pasos como se indica en la *figura 2.*

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

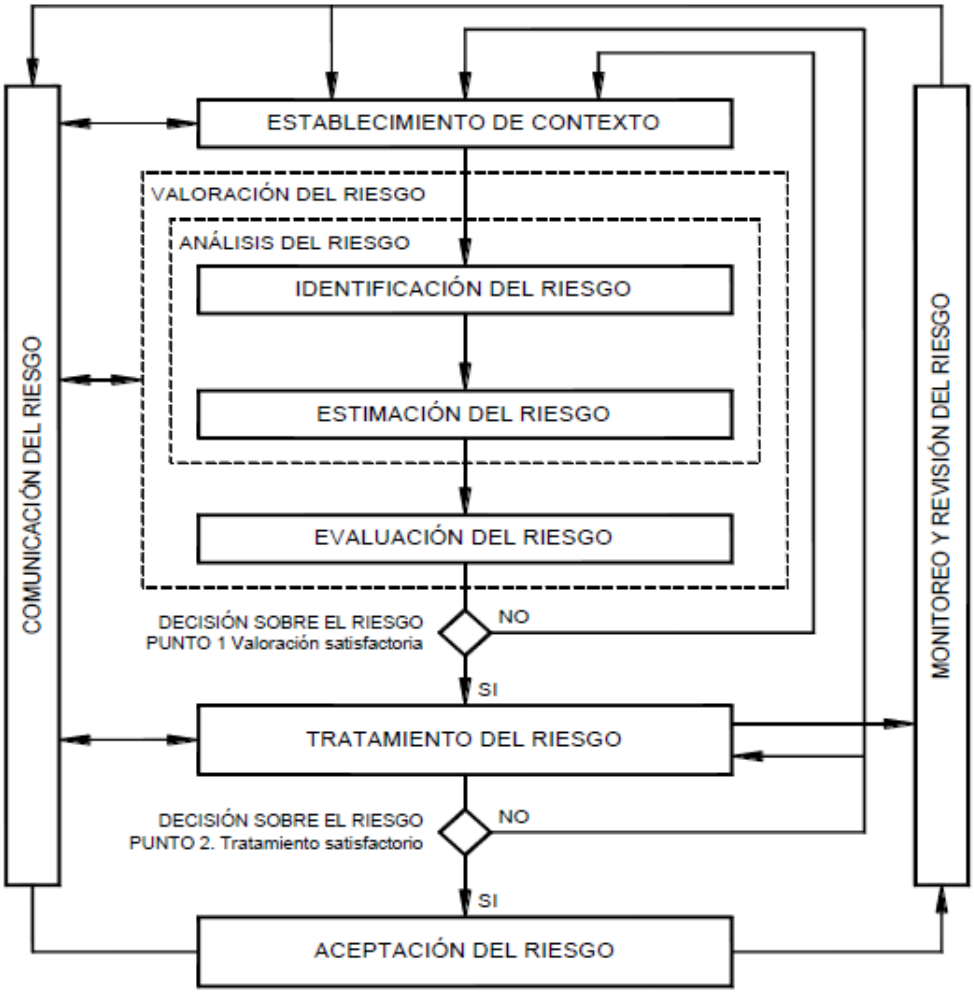

Figura 2. Proceso de Gestión de Riesgos de Seguridad de la Información

Fuente: MinTIC, "Guía de gestión de riesgos." 2016.

6.1 Establecimiento del Contexto

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la entidad.

El contexto interno considera factores que impactan directamente a:

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

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

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros • Flujos de información y los procesos de toma de decisiones • Empleados, contratistas • Objetivos estratégicos y la forma de alcanzarlos • La misión, visión, valores y cultura de la organización • Sus políticas, procesos y procedimientos • Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional • Roles y responsabilidades • Sistemas de información o servicios.	• Identificación de los procesos y su respectiva caracterización • Detalle de las actividades que se llevan a cabo en el proceso • Flujos de información • Identificación y actualización de los activos en la cadena de valor de la entidad pública • Recursos • Alcance del proceso • Relaciones con otros procesos de la entidad pública • Cantidad de ciudadanos afectados por el proceso • Procesos de gestión de riesgos que se tienen actualmente implementados • Personal involucrado en la toma de decisiones

Figura 3. Establecimiento del Contexto Interno

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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

CONTEXTO EXTERNO

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

Figura 4. Establecimiento del Contexto Externo.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

6.2 Análisis de riesgos

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden entorpecer el normal desarrollo de los procesos.

Un insumo vital para la identificación del riesgo es la clasificación de los activos de información, para la identificación de los riesgos de la Entidad se tomaron en cuenta los activos de información con nivel de criticidad ALTA, dado la importancia de la disponibilidad, confidencialidad e integridad de la información para las operaciones y la Entidad.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

En la Matriz de Riesgos, se contempla la identificación del riesgo basada en:

- Proceso: Unidad de análisis donde se evaluará el riesgo, es equivalente al proceso, área o unidad de negocio
- Objetivo del proceso: Objetivo del proceso
- Identificación de activos: Activos potencialmente afectados por los riesgos identificados
- Propiedad de la afectación principal de la amenaza: (confidencialidad, integridad, disponibilidad)
- Amenaza: Causa, evento o suceso que podría afectar el cumplimiento de los objetivos
- Vulnerabilidad: Debilidad o susceptibilidad de un activo o de un control que puede ser explotada por la amenaza
- Efecto de la materialización del riesgo: Consecuencia si la amenaza se aprovecha de la vulnerabilidad
- Descripción del riesgo: Descripción del riesgo en términos de: Qué (impacto - Consecuencia) + Cómo (causa inmediata - Amenaza) + ¿Por qué? (causa raíz - vulnerabilidad)

Para la identificación de los escenarios de riesgos de seguridad de la información se tomó como base el **catálogo de amenazas** establecido en la ISO /IEC 27005, identificando con ello el evento o suceso que podría afectar el cumplimiento de los objetivos en el activo de información identificado (daño físico, eventos naturales, pérdida de los servicios esenciales, perturbación debida a la radiación, compromiso de la información, fallas técnicas, acciones no autorizadas, compromiso de las funciones); es de aclarar, que algunas amenazas pueden afectar a más de un activo de información y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

Tabla 1. Catálogo de Amenazas Comunes establecidos en la ISO/IEC 27005

Tipo	**Nombre Amenaza**	**Origen** **A: Accidental** **D: Deliberadas** **E: Ambientales**
Acciones no autorizadas	Copia fraudulenta del software	D
	Procesamiento ilegal de los datos	D
	Uso de software falso o copiado	A, D

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Uso no autorizado del equipo	D
	Corrupción de los datos	D
	Virus Informático o Código Malicioso	A, D
Compromiso de la información	Datos provenientes de fuentes no confiables	A, D
	Detección de la posición	D
	Divulgación de información	A, D
	Escucha encubierta	D
	Espionaje remoto	D
	Hurto de equipo	D
	Hurto de medios o documentos	D
	Interceptación de señales de interferencia comprometedoras	D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Recuperación de medios reciclados o desechados	D
Compromiso de las funciones	Falsificación de derechos	D
	Incumplimiento en la disponibilidad del personal	A, D, E
	Negación de acciones	D
	Abuso de derechos o elevación de privilegios	A, D
	Error en el uso	A
	Modificación de la Información	A, D
Daño Físico	Accidente importante	A, D, E
	Contaminación	A, D, E
	Daño por agua, humedad o líquidos	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Fuego	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos Naturales	Fenómenos Climáticos	E
	Fenómenos Sismicos	E
	Fenómenos Volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Fallas Técnicas	Falla del equipo	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
	Mal funcionamiento del equipo	A
	Mal funcionamiento del software	A
	Saturación del sistema de información	A, D
Humanas	Cibercrimen	D
	Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	D
	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	D
	Pirata informático, intruso ilegal (Hacker, Cracker)	D
	Terrorismo, Sabotaje, Vandalismo	D
Pérdida de los servicios esenciales	Falla en el equipo de telecomunicaciones	A, D
	Falla del servicio de telecomunicaciones	A, D
	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Denegación del Servicio	D
Perturbación debida a la radiación	Impulsos electromagnéticos	A, D, E
	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E

Así mismo, se identificaron las **vulnerabilidades** (debilidades) que conllevan a que las amenazas se conviertan en situaciones de riesgos reales, teniendo en cuenta el **catálogo de vulnerabilidades** comunes de la ISO/IEC 27005. Es de aclarar, que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. A continuación, se presenta la relación entre las vulnerabilidades de acuerdo con el tipo de activos y amenazas.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Tabla 2. Vulnerabilidades por Tipo de Activos y Amenazas

Tipo	Nombre Vulnerabilidad	Amenaza
Hardware	Almacenamiento sin protección	Hurto de medios o documentos
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Copia no controlada	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
Información	Ausencia de copias de respaldo	Manipulación con software
	Clasificación inadecuada de la información	
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Lugar	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Red energética inestable	Pérdida del suministro de energía
	Ubicación en un área susceptible de inundación	Inundación

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Vulnerabilidad no evaluada	Eventos Naturales
Organización	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de política formal sobre la utilización de computadores o portátiles	Hurto de equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
Personal	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Entrenamiento insuficiente en seguridad	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Uso incorrecto de software y hardware	Error en el uso
Red	Arquitectura insegura de la red	Espionaje remoto
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Líneas de comunicación sin protección	Escucha encubierta
	Punto único de falla	Falla del equipo de telecomunicaciones
	Tráfico sensible sin protección	Escucha encubierta
	Transferencia de contraseñas	Espionaje remoto
Software	Asignación errada de los derechos de acceso	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Ausencia de documentación	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Configuración incorrecta de parámetros	Error en el uso

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Defectos bien conocidos en el software	Abuso de los derechos
	Descarga y uso no controlados de software	Manipulación con software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Fechas incorrectas	Error en el uso
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Interfaz de usuario compleja	Error en el uso
	Software ampliamente distribuido	Corrupción de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Tablas de contraseñas sin protección	Falsificación de derechos

Para la **identificación de las consecuencias** que la Entidad podría tener causadas por un escenario de riesgos (amenaza que explota una vulnerabilidad), se identificaron las siguientes:

Tabla 3. Consecuencias por Tipo de Riesgo

Consecuencia	Tipo Riesgo DAFP	Descripción
Pérdida estratégica	Riesgo Estratégico	Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia
Pérdida de imagen	Riesgo de Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución
Pérdida operativa o de servicio	Riesgo Operativo	Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional,

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias
Pérdida financiera	Riesgo Financiero	Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos excedentes de tesorería y el manejo de los bienes
Sanción legal	Riesgo de Cumplimiento	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad
Pérdida de capacidad tecnológica	Riesgo de Tecnología	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión
Daños	Riesgo Financiero	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Incumplimiento de los objetivos	Riesgo de Cumplimiento	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos

Fuente: Guía 7 de gestión de riesgos

Teniendo en cuenta la información obtenida en la fase de identificación del riesgo, se definieron los criterios de riesgo por niveles de **probabilidad,** posibilidad de ocurrencia del riesgo e **impacto**, consecuencias que pueden ocasionar a la organización aceptado por la Entidad.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Niveles de Probabilidad	Probabilidad	Valor	Frecuencia de la actividad
Raro	10%	1	Remoto. Evento que ocurre solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años
Improbable	25%	2	No esperado. Pero podría ocurrir algunas veces. Evento que ocurre al menos una vez en los últimos 5 años
Posible	50%	3	Posible. Se espera que no ocurra regularmente. Evento que ocurre al menos 1 vez en los últimos 2 años
Probable	75%	4	Mayor. Esperado que ocurre. Evento que ocurre al menos 1 vez en el último año
Casi Seguro	100%	5	Alta, certera. Evento que ocurre más de 1 vez al año

Figura 5. Criterios de Probabilidad

Se desarrollaron **criterios de impacto** del riesgo especificado en términos del grado de daño o costos para la Entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Perdidas de confidencialidad, integridad y disponibilidad de la información
- Perdida del negocio y valor financiero
- Daños para la reputación
- Operaciones deterioradas
- Incumplimiento de los requisitos legales

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Insignificante	1	10%	* Caída de sistemas y aplicativos claves resuelto en menos de 2 horas. * Sin pérdida de datos. * Sin afectación mayor a la confidencialidad, integridad y disponibilidad.	* Pérdida Financiera < 25 SMMLV * Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	* Difusión interna sólo a nivel de proceso o equipo de trabajo / Problemas resueltos antes de la cobertura por los medios de comunicación * Inquietudes por parte de colaboradores que no afectan el clima laboral * Ninguna afectación con organismos reguladores * No se afecta la imagen institucional de forma significativa.	* No hay afectación de la operación * No deriva en error u omisión * No hay interrupción de las operaciones de la entidad.	* No hay afectación * No se generan sanciones económicas o administrativas.
Menor	2	25%	* Caída de sistemas y aplicativos claves de máximo 2 horas * Sin pérdida de datos. * Afectación leve de al menos uno de los siguientes criterios (confidencialidad, integridad, y disponibilidad).	* Pérdida financiera Entre 25 y 50 SMMLV * Impacto que afecte la ejecución presupuestal en un valor ≥1%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor ≥1%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	* Difusión interna a nivel general en la empresa/ Problemas resueltos antes de la cobertura por los medios de comunicación Inquietudes por parte de colaboradores o proveedores que afecten el clima laboral de la organización * Observaciones o sanciones menores por el organismo regulador * Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	* Genera reprocesos menores, que afectan marginalmente la operación * Error u omisión al que se le puede dar un manejo interno * Interrupción de las operaciones de la entidad por algunas horas	* Acciones legales, acciones de no conformidad o violaciones normativas menores * Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.
Moderado	3	50%	* Caída de sistemas y aplicativos claves (entre 2 horas y 1 día). * perdida de datos. * Afectación moderada en dos de los siguientes criterios (confidencialidad, integridad y disponibilidad) * Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.	* Pérdida financiera entre Entre 50 y 100 SMMLV * Impacto que afecte la ejecución presu-puestal en un valor ≥5%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	* Cobertura adversa puntual en medios a nivel regional o local / Impacto apenas perceptible sobre la imagen de la empresa Inquietudes por parte de los grupos de interés * No conformidades o sanciones por el organismo regulador * Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.	* Riesgo pérdida de un contrato * Genera reprocesos moderados, dificultando la operación * Error u omisión sensible al que debe darse un manejo con contrapartes * Interrupción de las operaciones de la entidad por un (1) día. * Reproceso de actividades y aumento de carga operativa.	* Violación importante de la reglamentación, que genera una instrucción o un informe a las autoridades, con enjuiciamiento * Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. * Investigaciones penales, fiscales o disciplinarias.
Mayor	4	75%	* Caída de sistemas y aplicativos claves (>1 día) * Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. * Afectación grave a la confidencialidad, integridad y disponibilidad de la información.	* Pérdida financiera Entre 100 y 200 SMMLV * Impacto que afecte la ejecución presupuestal en un valor ≥20%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	* Cobertura adversa de amplia difusión en medios a nivel nacional / Impacto apreciable sobre la imagen de la empresa * Pérdida grave o disminución sensible del apoyo o credibilidad de algunos de los grupos de interés * Sanción mayor por el organismo regulador por incumplimientos graves * Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	* Genera reprocesos mayores, impidiendo o interrumpiendo parcialmente la operación * Error u omisión grave al que debe darse un manejo cuidadoso con contrapartes (Riesgo pérdida de un contrato) * Interrupción de las operaciones de la entidad por más de dos (2) días. * Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.	* Violación mayor de la reglamentación Litigios mayores * Sanción por parte del ente de control u otro ente regulador
Catastrófico	5	100%	* Caída sostenida de sistemas y aplicativos claves * Afectación muy grave a la confidencialidad, integridad y disponibilidad de la información. * Robo y/o Pérdida de información crítica para la entidad que no se puede recuperar.	* Pérdida financiera > 200 SMMLV * Impacto que afecte la ejecución presupuestal en un valor ≥50%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	* Cobertura adversa de amplia difusión en medios a nivel nacional, internacional o redes sociales. / Impacto significativo sobre la imagen de la empresa * Pérdida grave del apoyo o credibilidad de todos los grupos de interés (quejas y comentarios de los grupos de interés) * Intervención o cierre parcial o total por parte del Gobierno que impida la operación * Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	* Genera alto nivel de reprocesos, impidiendo o interrumpiendo totalmente la operación * Error u omisión severo que afecta seriamente la reputación de la organización con todas sus contraparte (Riesgo pérdida de varios contratos) * Interrupción de las operaciones de la entidad por más de cinco (5) días * Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.	* Acciones judiciales y multas significativas Litigios muy graves, incluidas "class actions" * Intervención por parte de un ente de control u otro ente regulador.

Figura 6. Criterios de impacto

Una vez realizada la evaluación cualitativa del cálculo de la **probabilidad X impacto**, se obtiene el **riesgo inherente** (sin evaluación de controles) en la *figura* se aprecia la matriz de calificación y evaluación y respuesta a los riesgos, así como las zonas de riesgo presentando las posibles formas de tratamiento del riesgo.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: 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

Figura 7. Matriz de Calificación, Evaluación y Respuesta a los Riesgos

Fuente: pág 32 Guía 7 de gestión de riesgos

6.3 Valoración del Riesgo

En esta etapa se evaluaron los controles existentes en la Entidad, para cada control se estableció su descripción, objetivo de control referenciado en el Anexo A del estándar ISO/IEC 27001:2013 y la efectividad de los controles; teniendo en cuenta las características relacionadas con la eficiencia y la formalización del control, en la tabla 4, se observa la descripción y el peso para cada uno.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Tabla 4. Atributos para Calificación del Control

Características		Descripción	Peso
Tipo	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
	Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	13%
	Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	5%
Implementación	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
	SemiAutomático	Controles involucrados en procesos que actúan parcialmente mediante tecnologías de información.	13%
	Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	5%
Documentación	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	25%
	Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	0%
Frecuencia	**Diario**	El control se aplica diariamente	25%
	Mensual	El control se aplica mensualmente	20%
	Trimestral	El control se aplica Trimestralmente	13%
	Anual	El control se aplica Anualmente	5%

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Una vez realizado la calificación del control (suma de pesos), se procede a realizar el cálculo de la probabilidad e impacto residual, teniendo en cuenta si el control afecta la probabilidad o impacto se desplaza en la matriz de calificación de evaluación y respuesta a los riesgos como se indica en la *figura 8.*

Rangos de Calificación de los Controles	Evaluación del Control	Dependiendo si el control afecta probabilidad o impacto se desplaza en la matriz de calificación. Evaluación y respuesta a los riesgos	
		Cuadrante a disminuir en la probabilidad	Cuadrante a disminuir en el impacto
Entre 0% - 50 %	Débil	0	0
Entre 51% - 75%	Moderado	1	1
Entre 76% - 100%	Fuerte	2	2

Figura 8. Rango de Calificación de los Controles

6.4. Tratamiento de Riesgos

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos, para lo cual se definen Medidas de Respuesta ante los Riesgos (asumir, reducir, compartir, trasferir o evitar), luego se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento).

Una vez identificados los riesgos que amenazan a la Entidad de acuerdo a los resultados obtenidos en la matriz de riesgo residual, se evalúan los controles actuales de la Entidad contra los controles del Anexo A de la norma ISO 27001:2013 que se deben aplicar para llevar a cada uno de los riesgos identificados a un nivel aceptable para la Entidad. Según la naturaleza del riesgo, las acciones que se pueden realizar para tratarlo pueden ser:

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

- Asumir el riesgo: En este escenario se decide no tratar el riesgo debido a no haber identificado controles adecuados para el tratamiento de los riesgos o haber identificado que el costo de implementar algún control es mayor que los beneficios que se obtendrán. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Seguridad de la Información indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves.

- Reducir el riesgo: Reducir los riesgos mediante la implementación de controles que reduzcan el riesgo a un nivel aceptable. Estos controles deberán presentar una documentación adecuada para su implementación y puesta en marcha.

- Evitar el riesgo: Esta opción corresponde a evitar la actividad o acción que da origen al riesgo, normalmente se utiliza cuando la evaluación del riesgo es muy alta, o los costos para implementar los controles exceden los beneficios de su implementación

- Transferir el riesgo: Alternativa más económica en caso de que sea muy costoso o difícil reducir o controlar un riesgo. Sin embargo, al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento.

6.5. Comunicación de Riesgos

Participan todos los procesos e involucran a todos los colaboradores para el levantamiento de los mapas de riesgo, contando con el aporte de los colaboradores con mayor experticia tanto para la identificación como para el tratamiento de riesgos.

Cuando se identifica un riesgo el INVAMA suministra, comparte u obtiene información a través de un diálogo con las partes involucradas con respecto a la gestión del riesgo. La información está relacionada con la existencia, la naturaleza, la forma, la probabilidad, el significado, la evaluación, la aceptabilidad y el tratamiento de la Gestión de riesgo.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

La revisión del plan de tratamiento de los riesgos y la evaluación del riesgo residual, debe ser aceptada por la alta dirección de manera formal.

La información obtenida sobre los riesgos debe ser comunicada al grupo directivo de la Entidad, con el fin de tener conocimiento y claridad de aquellos riesgos que ponen en peligro la seguridad y privacidad de la información en la organización y de alguna manera poder evitar o reducir la ocurrencia e impacto de las brechas de seguridad de la información, brindar soporte para la toma de decisiones y planificar las acciones necesarias.

6.6. Monitoreo - Información de Riesgos y revisión

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo a la criticidad del riesgo asociado, las responsabilidades del monitoreo comprenden todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos.
- Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios de riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.

La Entidad debe monitorear y revisar los factores de riesgos, con el fin de detectar cambios en el contexto interno y externo de la Entidad, incluyendo los cambios en los criterios del riesgo que exijan revisar el tratamiento de riesgos; asegurando así la mejora continua del proceso de gestión de riesgos de seguridad de la información.

6.7. Declaración de Aplicabilidad (SOA).

La norma ISO 27001:2013, exige como parte del establecimiento del SGSI, producir una declaración de aplicabilidad que contenga los controles seleccionados con su respectiva justificación. Estos controles son tomados del Anexo A de la norma ISO 27001:2013 y en la guía 8 del MinTic, los cuales brindan una serie de

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

controles y recomendaciones para el tratamiento de los riesgos en una organización.

La declaración de aplicabilidad del INVAMA, consta de ciento diez (110) controles que aplican a la Entidad, 4 de los controles no serán aplicados por tratarse de temas de desarrollo interno de software, la declaración de aplicabilidad contiene la siguiente información:}

- Dominio: Dominio al que pertenece el control
- Objetivo de Control: Es la descripción del control, en él se indica exactamente a que se refiere cada uno de los controles de la norma.
- Número Control: Identificador de cada uno de los controles propuestos.
- Código del Control: Identificador del control dentro de la norma.
- Control: Nombre del control, se hace referencia a un tema específico al que un riesgo puede estar asociado.
- Controles actuales: Identifica los controles actuales que tiene la Entidad para el dominio seleccionado.
- Aplica: Se indica si el control en mención es aplicable a la organización o si no lo es.
- Aspectos del control o Justificación la exclusión: La justificación de la aplicabilidad o no aplicabilidad del control en mención.
- Selección del control: Indica el motivo de selección del control. Por ser requisito legal, por mejora o buena práctica, por valoración / tratamiento del riesgo.
- Declaración de aplicabilidad: Acciones o actividades a llevar a cabo para la implementación del control.
- Dependencia o Responsable: Área o persona responsable de implementar el control.
- Estado del control: Define si está en estado Implementado, Sin Implementar, En Implementación.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

7. MAPA DE RUTA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

ACCIONES	RESPONSABLE	FECHA INICIO	FECHA FIN	RESULTADO
Actualizar política y metodología de gestión de riesgos.	- Responsable de Seguridad y Privacidad de la Información -Comité MIPG	01-Feb-2024	28-Feb-2024	Política y metodología
Socialización de la guía y herramienta de gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Responsable de Seguridad y Privacidad de la Información -Comunicaciones	01-Mar-2024	31-Mar-2024	Socialización
Identificación, análisis y evaluación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Responsable de Seguridad y Privacidad de la Información -Líderes de procesos	01-Abr-2024	30-Abr-2024	Matriz de Riesgos
Retroalimentación, revisión y verificación de los riesgos identificados (ajustes)	-Responsable de Seguridad y Privacidad de la Información -Líderes de procesos	01-May-2024	31-May-2024	Matriz de Riesgos
Aceptación, aprobación riesgos identificados y planes de tratamiento	-Responsable de Seguridad y Privacidad de la Información -Comité MIPG	01-Jun-2024	30-Jun-2024	Actas de Reunión Matriz de Riesgos

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Publicación y socialización matriz de riesgos	-Responsable de Seguridad y Privacidad de la Información -Comunicaciones	01-Jul-2024	31-Jul-2024	Link de Transparencia
Tratamiento de riesgos identificados	-Responsable de Seguridad y Privacidad de la Información	01-ago-2024	31-dic-2024	Matriz de Riesgos
Evaluación riesgos residuales	-Responsable de Seguridad y Privacidad de la Información	01-ago-2024	31-dic-2024	Matriz de Riesgos
Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	-Responsable de Seguridad y Privacidad de la Información -Líderes de procesos	01-ago-2024	31-dic-2024	Oportunidades de mejora
Generación, presentación y reporte de indicadores seguimiento de riesgos de seguridad y privacidad de la información	-Responsable de Seguridad y Privacidad de la Información	01-ago-2024	31-dic-2024	Informe de riesgos

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA MODIFICACIÓN
0	27-01-2021	Creación del documento
1	28-01-2022	Ajustes al documento
2	27-01-2023	Actualización del mapa de ruta acciones y resultados
3	21-01-2024	Actualización normativa, metodología, mapa de ruta

FIRMAS Y REVISIONES

	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	DIANA LORENA CORTÉS JIMÉNEZ	Técnico Administrativo Sistemas	21-01-2024	
APROBÓ	JAIRO ALFREDO LÓPEZ BAENA	Gerente	25-01-2024	

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co