Instituto de Educación Técnica Profesional
de Roldanillo, Valle - INTEP

Establecimiento Público Departamental
Nit. 891.902.811-0

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN- INTEP

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) ha establecido un Modelo Integrado de Gestión (MIG) y un Sistema Integrado de Gestión (SIG), según lo dispuesto en la Resolución 2175 del 22 de junio de 2022. Este modelo tiene como objetivo alinear las políticas y directrices de MIG con otros modelos y sistemas de gestión, como el MIPG, Responsabilidad Social Institucional y Seguridad y Privacidad de la Información, entre otros.

La implementación del MIG se basa en dimensiones y un eje articulador que responden a requisitos normativos, dinámicas organizacionales y la facilitación de la articulación de diversos modelos y sistemas. Se destaca la importancia de la política de Gobierno Digital, que incluye la Seguridad y Privacidad de la Información como habilitador y es responsabilidad de procesos como Fortalecimiento Organizacional, Gestión de TI y Seguridad y Privacidad de la Información.

En el Decreto 1008 de 2018, la seguridad de la información se define como un principio de la Política de Gobierno Digital, y el Decreto 767 de 2022 establece una estructura para la implementación de esta política, con énfasis en la seguridad y privacidad de la información como habilitador. Esto implica que el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP deba desarrollar capacidades y lineamientos de seguridad y privacidad en todos los procesos, trámites, servicios y sistemas de información para preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Además, el Decreto 2106 de 2019 exige que las autoridades cuenten con una estrategia de seguridad digital siguiendo las directrices del MINTIC. Esto se refuerza con la Resolución 500 de 2021, que establece lineamientos y estándares para la estrategia de seguridad digital y adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

En cumplimiento de estos decretos y resoluciones, se ha desarrollado este Plan de Seguridad y Privacidad de la Información en el INTEP, con el fin de cumplir con lo establecido en el Decreto 612 de 2018. Este documento debe ser aprobado por Comité Institucional de Gestión y Desempeño.

Es importante destacar que, en la evaluación de riesgos de seguridad de la información, un elemento fundamental es la clasificación de los activos de

información. Una práctica efectiva consiste en llevar a cabo la gestión de riesgos específicamente en aquellos activos de información que se encuentren clasificados como de nivel ALTO, de acuerdo con los criterios de Confidencialidad, Integridad y Disponibilidad.

Tabla 1 Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 2 Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

2. OBJETIVO

Establecer un enfoque integral para la gestión de riesgos de seguridad y privacidad de la información en el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital del MinTIC, la NTC/IEC ISO 27001, la Política Pública de Seguridad Digital y los criterios de continuidad de la operación de los servicios. El propósito principal es salvar los activos de información y fortalecer la confianza de los usuarios, ciudadanos, socios. y otras partes interesadas frente a ciberamenazas, garantizando la protección de la privacidad de la información, el manejo adecuado de medios, el control de acceso y la gestión de usuarios en el INTEP.

3. ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos de seguridad y privacidad de la información, realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el Ministerio/Fondo Único de TIC, se busca integrar buenas prácticas en los procesos del INTEP. Esto contribuirá a la toma de decisiones informadas y prevenir incidentes que puedan afectar el logro de los objetivos. En conjunto con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1], se establecen los lineamientos para identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el MINTIC. El Plan de Tratamiento de Riesgo considera especialmente los riesgos clasificados en los niveles Alto y Extremo de acuerdo con las directrices del Ministerio TIC.

Este documento se aplica a todo el modelo de operación por procesos del Ministerio/Fondo Único de TIC y se ajusta a lo establecido en el Decreto 612 de 2018, la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información, que se encuentra en línea con la norma NTC/IEC ISO 27001, y de estar en consonancia con la estrategia de Seguridad Digital del Estado colombiano.

El alcance de este plan de tratamiento de riesgos de seguridad y privacidad de la información se centra en los procesos de servicios de infraestructura tecnológica. Su objetivo principal es controlar y mitigar los riesgos de seguridad de la información institucional gestionada por la Oficina de Informática del INTEP.

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

4. RESPONSABILIDAD

los responsables de la gestión del riesgo en la entidad son los siguientes:

1. **Alta y media dirección:** Los directivos de alto y medio nivel son responsables de comprometerse con el proceso de administración de riesgos. Su compromiso es esencial para el éxito del proceso, ya que se necesita su aprobación y apoyo en la toma de decisiones relacionadas con la gestión de riesgos.

2. **Directivo de primer nivel:** Deben designar a un directivo de primer nivel que asesore y apoye todo el proceso de diseño e implementación del Componente de Gestión de Riesgos. Preferiblemente este directivo debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del MECI (Modelo Estándar de Control Interno) y el Sistema de Gestión de la Calidad.

3. **Equipo MECI o grupo interdisciplinario:** La conformación de un equipo MECI o un grupo interdisciplinario es esencial para abordar integralmente los riesgos y tener una visión completa del INTEP. Este equipo debe incluir representantes de diferentes áreas de la organización y se encargará de analizar los riesgos en diversos procesos.

4. **Equipo de proyecto MSPI**: Se menciona que el equipo interdisciplinario que se encarga de analizar los riesgos de seguridad debe estar integrado por algunos de los integrantes del proyecto MSPI (Modelo de Seguridad y Privacidad de la Información). Esto garantiza un contexto organizacional completo en el desarrollo del MSPI.

Por lo tanto, la alta y media dirección, el directivo de primer nivel, el equipo MECI o grupo interdisciplinario y el equipo de proyecto MSPI son los responsables clave en la gestión de riesgos y seguridad de la información en el Instituto de Educación

Técnica Profesional de Roldanillo Valle - INTEP. Cada uno desempeña un papel importante en el proceso de administración de riesgos y en la implementación de medidas de seguridad y privacidad de la información

5. NORMATIVIDAD

- **Constitución Política de Colombia**. Artículos 15, 20, 23 y 74.
- **Ley 2088 de 2012**. Por la cual se regula el trabajo en casa y se dictan otras disposiciones
- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país.
- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1450 de 2011**. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC Se crea la agencia Nacional de espectro

y se dictan otras disposiciones.

- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **Ley 594 de 2000.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 44 de 1993**. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 23 de 1982.** Sobre derechos de autor
- **Decisión Andina 351 de 1993**. Régimen común sobre derecho de autor y derechos conexos
- **Decreto 338 de 2022**. Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información

y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea

- **Decreto 1287 de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Decreto 620 de 2020**. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 728 de 2017**. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- **Decreto 103 de 2015**. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1068 de 2015**. Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.

- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 886 de 2014**. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1377 de 2013**. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 2364 de 2012**. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 884 de 2012** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Resolución 0448 de 2022**. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.
- **Resolución 1838 de 2022**. Por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019.
- **Resolución 746 de 2022**. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
- **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 como habilitador de la Política de Gobierno Digital

- **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.
- **Resolución 924 de 2020**. Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2007 de 2018.
- **CONPES 3995 de 2020**. Confianza y Seguridad Digital
- **CONPES 3854 de 2017**. Política Nacional de Seguridad digital.
- **CONPES 3701 de 2011**. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **Directiva 26 de 2020**. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

6. DEFINICIONES

En este espacio se listan algunas definiciones que utilizaremos en el desarrollo del plan de tratamiento de riesgos de la información del Instituto de Educación Técnica Profesional de Roldanillo Valle – INTEP.

A

E

F

G

R

S

T

U

7. DOCUMENTOS ASOCIADOS

- MIG-TIC-MC-001 Manual del MIG[2]
- SPI-TIC-MA-001 Manual de Políticas de Seguridad y Privacidad de la Información[3]
- MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI de la política de Gobierno Digital del MinTIC.[4]

8. VISION GENERAL DEL PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

2 https://www.mintic.gov.co/images/documentos/documentos_comentarios/manual-calidad.docx
3 https://www.mintic.gov.co/portal/715/articles-2627_resolucion_0448_2022.pdf
4 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Proceso para la administración del riesgo:

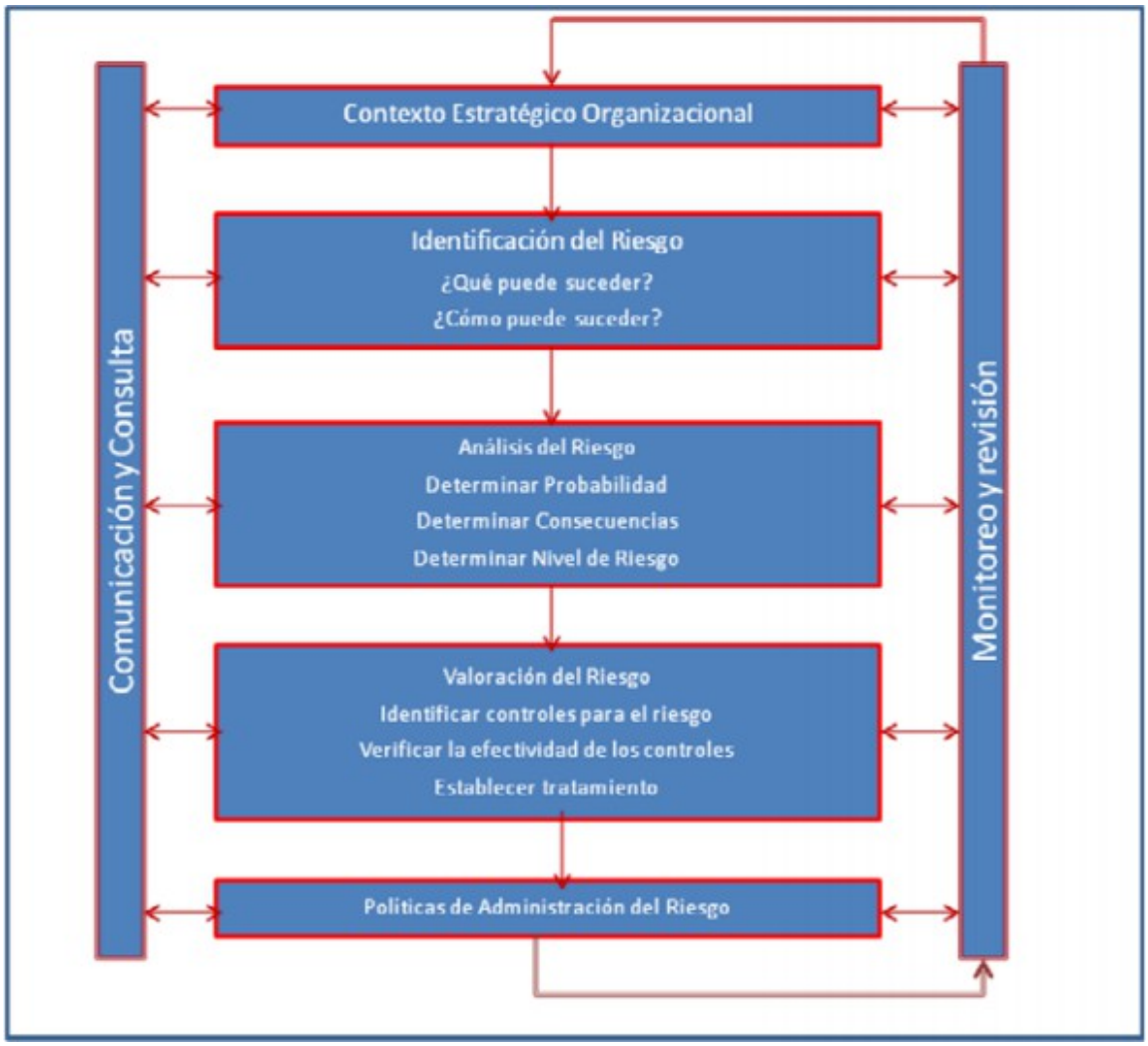

Ilustración 1 Tomado de la Cartilla de Administración de Riesgos del DAFP[5]

5 https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

- **Proceso para la administración del riesgo en seguridad de la información**

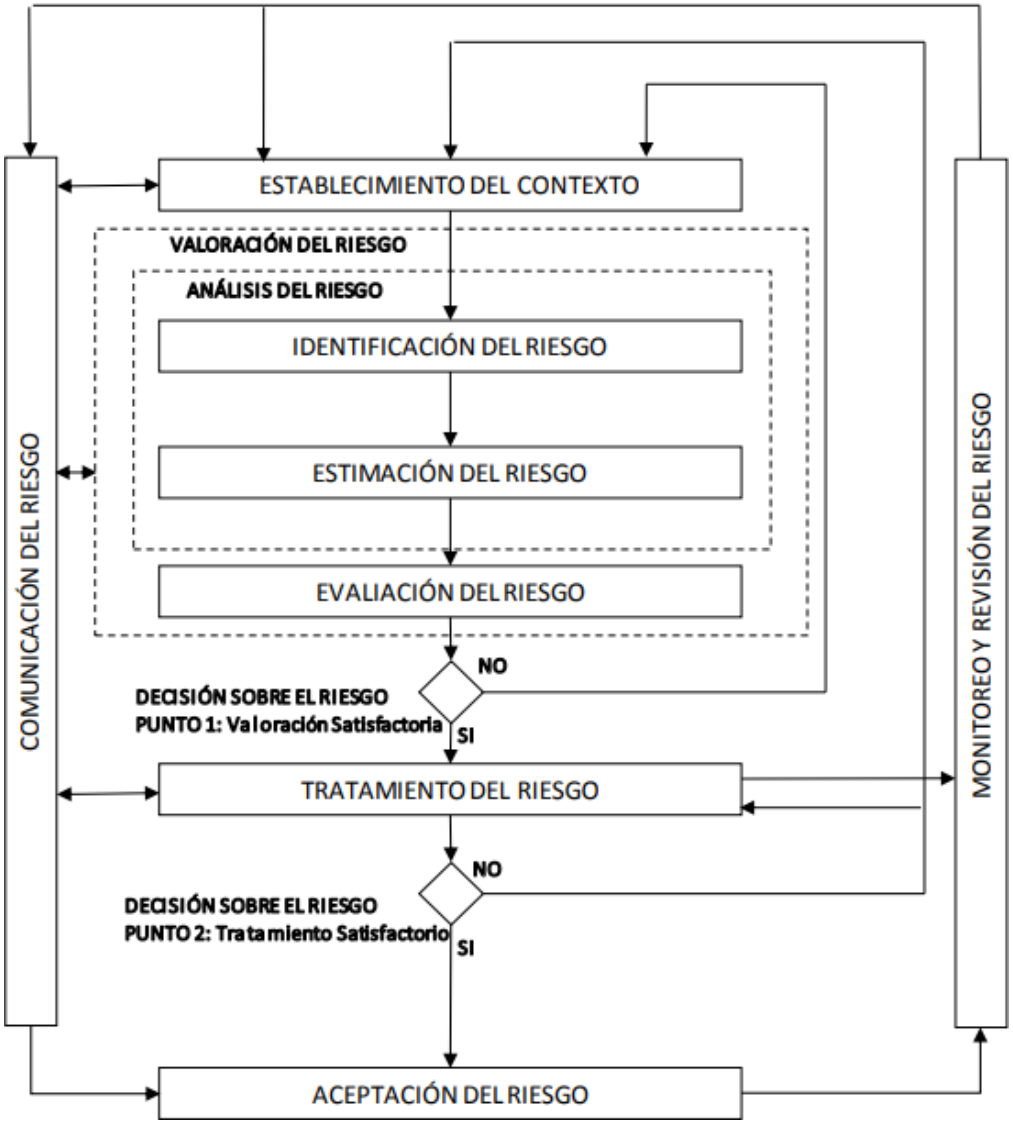

Ilustración 2 Tomado de la NTC - ISO / IEC 27005[6]

[6]https://www.studocu.com/latam/document/universidad-bolivariana-de-venezuela/especializacion-en-seguridad-industrial/iso-27005-norma-iso/33809431

La valoración y tratamiento del riesgo son aspectos fundamentales en la gestión de la seguridad de la información. La valoración del riesgo es una herramienta clave para identificar las amenazas y vulnerabilidades que pueden afectar la seguridad de la información, permitiendo la identificación de los activos de información críticos, las amenazas y vulnerabilidades asociadas, y el impacto potencial de un incidente de seguridad. De esta manera, se pueden establecer medidas de tratamiento del riesgo adecuadas para minimizar los riesgos identificados y garantizar la protección de la información.

Una vez realizada la valoración del riesgo, se pueden determinar las acciones necesarias para reducir los riesgos a un nivel aceptable. Estas acciones pueden incluir la implementación de medidas de seguridad, tales como la adopción de políticas de seguridad de la información, la realización de auditorías de seguridad y la adopción de normas y regulaciones en materia de seguridad de la información. De esta manera, se pueden establecer controles de seguridad adecuados para minimizar los riesgos identificados y garantizar la protección de la información. Es importante destacar que la implementación de estas medidas debe ser continua y estar en constante revisión para asegurar su efectividad y adaptación a los cambios en el entorno de la organización.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

Tabla 3 Etapa de la Gestión del Riesgo a lo largo del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

El plan de tratamiento de riesgos de seguridad y privacidad de la información propone una gestión iterativa en cuanto a las actividades de valoración del

impacto y tratamiento de los riesgos identificados. Esto implica que el proceso de gestión de riesgos es un ciclo continuo que requiere una revisión y actualización constante para garantizar su efectividad. De esta manera, se pueden identificar y evaluar los riesgos de manera periódica, y establecer medidas de tratamiento adecuadas para minimizarlos. La gestión iterativa del plan de tratamiento de riesgos permite una mejora continua en la gestión de la seguridad y privacidad de la información, asegurando la protección de los activos de información críticos de la organización.

8.1 Establecimiento del Contexto para la Gestión de Riesgos de Seguridad de la Información

El contexto de gestión de riesgos de seguridad de la información establece los criterios básicos necesarios para enfocar el ejercicio de gestión de riesgos del Instituto de educación técnica profesional de Roldanillo – Valle INTEP y obtener los resultados esperados. Esto se logra mediante la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos del INTEP, el análisis de las debilidades y amenazas asociadas, la valoración de los riesgos en términos de sus consecuencias para la Entidad y la probabilidad de su ocurrencia, así como la construcción de acciones de mitigación para lograr y mantener niveles de riesgos aceptables para la Entidad. De esta manera, se pueden establecer medidas de seguridad adecuadas para minimizar los riesgos identificados y garantizar la protección de la información crítica de la organización. Es importante destacar que la gestión de riesgos debe ser un proceso continuo y estar en constante revisión para asegurar su efectividad y adaptación a los cambios en el entorno de la organización.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

8.1.1 Criterios de evaluación de riesgo de seguridad de la información

Los criterios de evaluación de riesgo de seguridad de la información se enfocan en varios aspectos clave:

- En primer lugar, se considera el valor estratégico del proceso para el INTEP.
- En segundo lugar, se evalúa la criticidad de los activos de información involucrados.
- Tercero, se toman en cuenta los requisitos normativos, legales y reglamentarios, así como las obligaciones contractuales.
- También se considera la importancia de la disponibilidad, integridad y confidencialidad para las operaciones del INTEP.
- Por último, se evalúan las expectativas y percepciones de las partes interesadas y las posibles consecuencias negativas para el buen nombre y reputación del instituto.

Al considerar estos criterios de evaluación de riesgos, se pueden identificar y evaluar los riesgos de manera efectiva y establecer medidas de tratamiento adecuadas para minimizarlos. Es importante destacar que la evaluación de riesgos debe ser un proceso continuo y estar en constante revisión para asegurar su efectividad y adaptación a los cambios en el entorno de la organización.

8.1.2 Criterios de impacto

Los criterios de impacto deben ser especificados en términos del grado de daño o costos que puedan ser causados al INTEP por un evento de seguridad de la información. Es importante considerar aspectos como:

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

8.1.3 Criterios de aceptación

En cuanto a los criterios de aceptación, es importante tener en cuenta las políticas, metas y objetivos del INTEP y de las partes interesadas. Estos criterios deben ser establecidos de manera dinámica e iterativa, y se deben revisar periódicamente para asegurar su eficacia. Es recomendable desarrollar escalas de aceptación del riesgo que permitan una evaluación clara y precisa de los riesgos asociados a la seguridad de la información.

8.2 Valoración de los riesgos de seguridad de la información

Antes de realizar la valoración de los riesgos de seguridad de la información, es importante determinar si es necesario identificar un inventario de activos de información de los procesos, ya que esto será la base del enfoque de la valorización de los riesgos de seguridad de la información. Es necesario identificar, describir y priorizar los activos de información cuantitativa o cualitativamente, teniendo en cuenta los criterios de evaluación del riesgo y los objetivos relevantes para la Institución. De esta manera, se podrá realizar una valoración precisa y efectiva de los riesgos asociados a la seguridad de la información.

Esta fase consta de las siguientes etapas:

- Análisis del riesgo: Identificación y estimación del riesgo.
- Evaluación del riesgo

8.2.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información, como primera medida se deberán identificar los activos de información por proceso evaluado.

Los activos de información se clasifican en:

- **Primarios**:

Es importante identificar los **procesos o subprocesos y actividades del negocio** que son críticos para la misión de la organización, ya que su pérdida o degradación pueden hacer imposible llevar a cabo dicha misión. También se deben considerar los procesos que contienen información confidencial o tecnología propietaria, aquellos que, si se modifican, pueden afectar significativamente el cumplimiento de la misión de la organización, y aquellos que son necesarios para cumplir con los requisitos contractuales, legales o reglamentarios. De esta manera, se podrá identificar y proteger adecuadamente los procesos más importantes para la organización.

Es fundamental identificar y proteger **la información** crítica para la ejecución de la misión o el negocio de la organización, así como la información personal que se encuentra protegida por las leyes de privacidad. También se deben considerar la información estratégica necesaria para alcanzar los objetivos establecidos por las orientaciones estratégicas de la organización, así como la información de alto costo que requiere un largo periodo de tiempo y/o un alto costo de adquisición para su recolección, almacenamiento, procesamiento y transmisión. Es importante tener en cuenta que existen otros tipos de información que también pueden ser críticos para la organización, por lo que se recomienda realizar una evaluación exhaustiva de los diferentes tipos de información que maneja la institución.

Para mejorar la gestión de riesgos en una entidad, es importante identificar y evaluar los **procesos y actividades de negocio** que son críticos para la organización. Estos pueden incluir aquellos relacionados con la propiedad intelectual, aquellos que, si se degradan, hacen imposible la ejecución de las tareas de la entidad, y aquellos necesarios para el cumplimiento legal o contractual, entre otros. Al identificar estos procesos y actividades críticos, se pueden establecer medidas de seguridad adecuadas para minimizar los riesgos identificados y garantizar la protección de la información crítica de la organización.

- **De Soporte**

Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

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

Estructura organizativa: responsables, áreas, contratistas, etc.

Es fundamental identificar y evaluar las amenazas que pueden causar daño a los activos, procesos y soportes de la organización. Para ello, se pueden realizar consultas a los dueños de los activos, usuarios y expertos en la materia, entre otros. Al identificar y valorar estas amenazas, se pueden establecer medidas de seguridad adecuadas para minimizar los riesgos identificados y garantizar la protección de la información crítica de la organización.

El siguiente paso revisar las **vulnerabilidades** que puedan ser aprovechadas por las amenazas para causar daños a los activos de información de la organización. Este paso se realiza después de haber identificado el listado de activos, las amenazas relacionadas y valorado los daños potenciales, y haber revisado las medidas de seguridad implementadas. Al revisar las vulnerabilidades, se pueden establecer medidas de seguridad adicionales para minimizar los riesgos identificados y garantizar la protección de la información crítica del Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP.

Entre los diferentes métodos que podemos utilizar estarían:

- Realizar entrevistas con los líderes de procesos y también con los usuarios.
- Realizar inspecciones periódicas en sitio.
- Utilizar herramientas para escaneo automatizado.

Por cada **amenaza** identificada analizaremos las **vulnerabilidades** que pudiesen ser explotadas.

Como paso final, se identificarán las **consecuencias** que no son más que la manera como estas **amenazas** y **vulnerabilidades** afectan la integridad, disponibilidad y confidencialidad de los activos de información.

8.2.2 Estimación del riesgo

Una estimación del riesgo que permita establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias. Esta evaluación se realiza con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos, lo que permitirá a la institución tomar decisiones informadas sobre cómo manejar los riesgos identificados.

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

Lo más recomendable es realizar el análisis contando con el apoyo de las personas que se encuentren más familiarizadas con el proceso para determinar con mayor precisión el impacto y la probabilidad del riesgo y así poder clasificarlos en los rangos que sean establecidos.

Para estimar el riesgo desde el enfoque del impacto y las consecuencias, se deben

tomar en cuenta factores tales como pérdidas financieras, costos de reparación o reemplazo de activos de información, disminución del rendimiento, interrupciones en la actividad normal de la institución, multas o sanciones a consecuencia de la materialización del riesgo, daños personales, entre otros. La evaluación de estos factores permitirá establecer una valoración más precisa del riesgo y su impacto en la organización, lo que a su vez permitirá tomar decisiones informadas sobre cómo manejar los riesgos identificados.

Es esencial medir tanto las posibles consecuencias como la probabilidad de que ocurran situaciones que puedan impactar los activos de información del INTEP, alterar su normal operación o detenerla por completo. La medición y/o estimación de la probabilidad permitirá establecer una valoración más precisa del riesgo y su impacto en la organización, lo que a su vez permitirá tomar decisiones informadas sobre cómo manejar los riesgos identificados.

Formato para el registro, estimación y tratamiento de los riesgos de seguridad de la información

8.2.3 Formato para el registro, estimación y tratamiento de los riesgos de seguridad de la información.

El formato utilizado por el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP para registrar y dar tratamiento a los riesgos de los activos de información, es fundamental apoyarse del anexo B de la Norma Técnica Colombiana NTC-ISO/IEC 27005[7]

Este formato será diligenciado por los miembros de cada oficina, facultad o departamento y deberán calificar el impacto y la probabilidad de ocurrencia de cada riesgo identificado, así como también se brindan campos para determinar los planes de mitigación.

Para la estimación de los riesgos se utilizarán los siguientes criterios:

Tabla 4 CRITERIOS PARA CALIFICAR LA PROBABILIDAD

PROBABILIDAD			
CLASIFICACIÓN	**VALOR**	**DESCRIPCIÓN**	**FRECUENCIA**
Casi Seguro	5	Se espera su ocurrencia en la mayoría de las circunstancias	Más de 1 vez en al año
Probable	4	El evento probablemente ocurriría en la mayoría de las circunstancias	Al menos 1 vez en el último año
Posible	3	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
Improbable	2	Es poco probable que el evento se presente	Al menos 1 vez en los últimos 5 años
Rara Vez	1	El evento puede ocurrir solo en circunstancias excepcionales	No ha ocurrido en los últimos 5 años

[7] https://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

Adaptado para el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

Tabla 5 CRITERIOS PARA CALIFICAR EL IMPACTO

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	Impacto que afecte la ejecución presupuestal en un ≥50%. - valor - 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.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

MAYOR	- 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.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	Impacto que afecte la ejecución presupuestal 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	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los

	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.	entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.

MENOR	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 presupuesto total de la entidad en un valor ≥1%. - Impacto que afecte la ejecución presupuestal en un proceso. - 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.	- 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.

INSIGNIFICANTE	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.	- 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.

Adaptado para el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

Tabla 6 CRITERIOS PARA CALIFICAR EL IMPACTO-RIESGOS DE SEGURIDAD DIGITAL

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	-Afectación ≤ 2% de la población. -Afectación ≤ 1% del presupuesto anual de la entidad. No hay afectación medioambiental.	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad.

MENOR	2	-Afectación ≤ 10% de la población. -Afectación ≤ 2% del presupuesto anual de la entidad. -Afectación leve del medio ambiente requiere de ≤ 8 días de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad.

MODERADO	3	-Afectación ≤ 20% de la población. -Afectación ≤ 5% del presupuesto anual de la entidad. -Afectación leve del medio ambiente requiere de ≤ 8 semanas de recuperación.	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la Confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	-Afectación ≤ 30% de la población. -Afectación ≤ 20% del presupuesto anual de la entidad. -Afectación importante del medio ambiente que requiere de ≥6 meses de recuperación.	-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

CATASTRÓFICO	5	-Afectación ≥ 30% de la población. -Afectación ≥ 20% del presupuesto anual de la entidad. -Afectación muy grave del medio ambiente que requiere de ≥1 años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Adaptado para el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

8.2.4. Determinación del Riesgo Inherente y Residual

El análisis de riesgos, que se basa en la probabilidad e impacto, nos brinda una evaluación inicial del riesgo inherente y nos ayuda a comprender el nivel de exposición al riesgo que enfrenta el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP. La exposición al riesgo se determina mediante la ponderación de la probabilidad y el impacto, y se visualiza claramente en una matriz de riesgos, una herramienta que ilustra las áreas de riesgo y simplifica la evaluación inicial en un formato gráfico. Esto nos permite un análisis global de los riesgos en función de su ubicación en las diferentes zonas de la matriz, lo que a su vez facilita la priorización de acciones y la planificación de estrategias para el tratamiento de riesgos.

Tabla 7 Matriz de Calificación, Evaluación y respuesta a los Riesgos

PROBABILIDAD		IMPACTO					ZONA	NIVEL DE RIESGO
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO		
RARA VEZ	1	Zona1 de riesgo bajo- asumir el riesgo	Zona4 de riesgo bajo- asumir el riesgo	Zona8 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona15 de riesgo Alta Reducir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona17 de riesgo Alta Reducir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	ZONA RIESGO BAJA	Z-1
								Z-2
								Z.3
								Z-4
								Z-5
IMPROBABLE	2	Zona2 de riesgo bajo- asumir el riesgo	Zona5 de riesgo bajo- asumir el riesgo	Zona9 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona16 de riesgo Alta Reducir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona22 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	ZONA DE RIESGO MODERADO	Z-6
								Z-7
								Z-8
								Z-9
POSIBLE	3	Zona3 de riesgo bajo- asumir el riesgo	Zona7 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona13 de riesgo Alta Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona19 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona23 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	ZONA DE RIESGO ALTA	Z-10
								Z-11
								Z-12
								Z-13
								Z-14
								Z-15
PROBABLE	4	Zona6 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona11 de riesgo Alta Reducir ir el riesgo	Zona14 de riesgo Alta Reducir ir el riesgo Evitar el riesgo	Zona20 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo	Zona24 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo		Z-16
								Z-17
							ZONA DE RIESGO EXTREMA	Z-18
								Z-19
								Z-20

			Evitar el riesgo Compartir o trasladar el riesgo	Compartir o trasladar el riesgo	Compartir o trasladar el riesgo	Compartir o trasladar el riesgo		
CASI SEGURO	5	Zona10 de riesgo Alta Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona12 de riesgo Alta Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona18 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona21 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona25 de riesgo Extrema Reducir ir el riesgo Evitar el riesgo Compartir o trasladar el riesgo		Z-21 Z-22 Z-23 Z-24 Z-25

Esquema general de la Matriz de Riesgos Institucional y zonas de riesgo Institucional para el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP-Adaptado para el INTEP de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

Cada zona de riesgo viene identificada con un color distintivo que indica la severidad del riesgo de la siguiente manera:

Tabla 8 Zonas de Riesgo

Zona de Riesgo
B: Zona de riesgo Baja (Color Verde): 5 zonas, siendo Z- 5 la zona de mayor riesgo.
M: Zona de riesgo Moderada (color Amarillo): 4 zonas, siendo Z- 9 la zona de mayor riesgo.
A: Zona de riesgo Alta (Color Rojo): 8 zonas, siendo Z- 17 la zona de mayor riesgo.
E: Zona de riesgo Extrema (Color Vino tinto): 8 zonas, siendo la Z-25 la de más alto riesgo.

8.2.4 Evaluación de Riesgos

Una vez que hayamos evaluado minuciosamente los impactos, las probabilidades y las posibles consecuencias de los riesgos identificados en cada escenario de

incidentes, procederemos a determinar los niveles de riesgo. Estos niveles de riesgo serán sometidos a una comparación contextual, lo cual resultará en una toma de decisiones efectiva y pertinente, basada en los riesgos de seguridad de la información y considerando su potencial impacto en el Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP.

8.3 Tratamiento de los riesgos de seguridad de la información

Después de completar la fase de evaluación de riesgos, se genera una lista jerarquizada de riesgos o se elabora una matriz que visualiza los niveles de riesgo, determinados por su ubicación y código de color. Posteriormente, se procede a la selección de una o más estrategias de tratamiento de riesgos en consonancia con su evaluación y los criterios definidos en el marco de gestión de riesgos.

Para cada nivel de riesgo identificado, se llevará a cabo una elección individualizada de la estrategia de tratamiento más adecuada. En la toma de decisiones, el factor crítico será el análisis costo-beneficio del tratamiento, priorizando la eficiencia económica y el valor obtenido en relación con la inversión requerida.

Tabla 9 RELACION COSTO BENEFICIO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

OPCION DE TRATAMIENTO	COSTO-BENEFICIO
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 nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios.
Trasladar o **compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).	El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo
Reducir el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto	El costo y el tiempo del tratamiento es adecuado a los beneficios

Aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa	La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.

El resultado de esta fase será un plan de tratamiento de riesgos que contiene la selección y justificación de una o más opciones para cada uno de los riesgos identificados, identificando además los riesgos residuales, es decir, aquellos que continúan existiendo a pesar de las medidas tomadas.

8.4 Monitoreo y Seguimiento a los Riesgos de seguridad de la información

Se llevará a cabo una revisión periódica y sistemática de los activos, vulnerabilidades, probabilidades, impactos y amenazas con el fin de detectar posibles cambios que puedan requerir una valoración constante y continua de los riesgos en materia de seguridad de la información.

Es importante destacar que los riesgos evolucionan en consonancia con las modificaciones en los procesos del Instituto de Educación Técnica Profesional de Roldanillo Valle - INTEP, y estos cambios pueden manifestarse de manera imprevista. Por tanto, resulta esencial realizar una supervisión continua para identificar aspectos tales como la incorporación de nuevos activos o ajustes en su valor, la aparición de nuevas amenazas, la identificación de nuevas vulnerabilidades o modificaciones en las ya conocidas, variaciones en la gravedad de los impactos, y, por último, la ocurrencia de nuevos incidentes relacionados con la seguridad de la información.

En este sentido, es imperativo establecer esquemas de seguimiento y medición en el sistema de gestión de riesgos de seguridad de la información, con el propósito de contextualizar las decisiones de manera oportuna y basada en información actualizada.

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORO	REVISO	APROBO
01	02 DIC 2025	Ing. Ricardo Buitrago Umaña	Dr. Duberney Preciado Rodríguez	Dr. Duberney Preciado Rodríguez