Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025

Oficina de Gestión TIC

UNIPAZ®
Instituto Universitario de la Paz

Tabla de contenido

Lista de Tablas

Lista de figuras

1. INTRODUCCIÓN

Teniendo en cuenta la necesidad de Administrar de manera optimizada los riesgos de las Instituciones Públicas, el Instituto Universitario de la Paz - UNIPAZ, ha establecido el siguiente plan para la administración del riesgo y diseño de controles de seguridad digital de acuerdo con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones – Min. TIC.

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misión del Instituto Universitario de la Paz - UNIPAZ. Por lo tanto, se deben implementar los controles necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior del Instituto Universitario de la Paz - UNIPAZ.

Este documento tiene en cuenta el contexto, las necesidades de la institución, las buenas prácticas y la normatividad vigente como: la NTC (Norma Técnica Colombiana) ISO 27001:2013, ISO 27701:2020, ISO 22301:2019, lo establecido en el Decreto 1008 de 14 de junio 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”, la Resolución 1519 de 2022 “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” y 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 como habilitador de la política de Gobierno Digital” dentro del cual se establecen para las entidades del estado los Habilitadores Transversales: Seguridad de la Información, Arquitectura de TI y Servicios Ciudadanos Digitales.

El presente Plan de Gestión de Riesgos de Seguridad Digital inicia con la definición del contexto de los riesgos de seguridad digital a los que está expuesta la institución, dando cubrimiento a los procesos estratégicos, misionales, de evaluación, y de apoyo, y concluye con el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

2. OBJETIVO GENERAL

Establecer un marco de gestión de riesgos de seguridad digital a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información, con el fin de lograr niveles de aceptación razonable del riesgo, en relación con los atributos de disponibilidad, integridad y confidencialidad de la información del Instituto Universitario de la Paz - UNIPAZ.

2.1. Objetivos Específicos

- Fortalecer y optimizar la gestión de seguridad y privacidad de la información al interior del Instituto Universitario de la Paz - UNIPAZ, apoyando el cumplimiento de los objetivos estratégicos de la entidad.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.
- Identificar, clasificar y mantener actualizados los activos de información de la institución.
- Reportar y gestionar los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de manera oportuna y pertinente reduciendo su impacto y propagación.
- Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos en los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.
- Fortalecer la cultura, el conocimiento y las habilidades del personal Directivo, Administrativo y Docentes, en los temas de seguridad y privacidad de la información en el Instituto Universitario de la Paz - UNIPAZ.
- Desarrollar estrategias que permitan la continuidad de los servicios tecnológicos prestados por la institución, frente a situaciones adversas que impidan el normal funcionamiento y prestación de estos.

3. ALCANCE

El presente plan describe las actividades necesarias para llevar a cabo la identificación de riesgos de seguridad digital sobre los activos de información, la creación de controles y planes de mejora con su debido seguimiento para aplicar el correspondiente tratamiento de riesgos enmarcado en las siguientes categorías:

Aceptar el riesgo: la institución decide después de un análisis no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Esta opción se puede considerar para riesgos con nivel bajo, sin embargo, se pueden presentar riesgos con otro nivel a los cuales la entidad no puede aplicar controles o planes para reducir el riesgo y es necesario aceptarlo. La aceptación del riesgo no implica que se olvide, sino que se debe hacer un seguimiento continuo del mismo.

Reducir el riesgo: se generan controles y/o planes de mejora que permitan reducir la probabilidad y/o el impacto del riesgo, estos controles están relacionados con la implementación de la ISO/IEC 27002, los cuales permiten una segregación de funciones, registros, entre otros que permitan la reducción prevista sobre el riesgo.

Evitar el riesgo: en este caso la institución deja de realizar las actividades que dan lugar al riesgo.

Compartir el riesgo: en este caso existen dos maneras de compartir el riesgo y es tercerizar la operación de la actividad que conlleva la probabilidad del riesgo y la otra manera es por medio de la adquisición de un seguro.

4. DEFINICIONES O SIGLAS

Para la adecuada gestión de riesgos de seguridad digital se debe manejar con propiedad los siguientes términos:

Activo: [Según **ISO 27000**]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: [Según **ISO 27000**]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis del riesgo: [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.

Consecuencia: [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

Controles: [Según ISO 27000]: 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática

Criterios del riesgo: [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Evaluación del riesgo: [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Identificación del riesgo: [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: [Según ISO 27000]: El coste para la empresa 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.

Inventario de activos: [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

Nivel de riesgo: [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

Perfil del riesgo: [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.

Política: [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

Política: para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Reducción del riesgo: [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

Riesgo: [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

Vulnerabilidad: [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO

Tabla 1 Marco normativo

NORMA	FECHA	CONTEXTO
Directiva Presidencial 02	Febrero 24 de 2022	“Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”
Decreto 338	Marzo 8 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"
Resolución 746	Marzo 11 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".
Decreto 767	Mayo 16 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”
Directiva Presidencial 03	Marzo 15 de 2021	Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos.
Resolución 500	Marzo 10 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".
Conpes 3995	Julio 1 de 2020	Política Nacional de Confianza y Seguridad Digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”

NORMA	FECHA	CONTEXTO
Resolución 1519	Agosto 24 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 en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”
Guía para la administración del riesgo y el diseño de controles en entidades públicas -V5	Diciembre de 2020	Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.
Decreto 612	Abril 4 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 1008	Junio 14 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Tí-tulo 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1915	Julio 12 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.
Resolución 2140	Octubre 19 de 2017	"Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones"
Conpes 3854	Abril 11 de 2016	Política Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
Decreto 103 de 2015	Enero 20 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1068	Mayo 26 de 2015	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581

NORMA	FECHA	CONTEXTO
		de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Capítulo 26.
Ley 1712	Marzo 06 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.
Decreto 886	Mayo 13 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 1377	Junio 23 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581	Octubre 17 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.
Ley 1273	Enero 05 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.

6. IMPLEMENTACIÓN DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La comunicación sobre el riesgo es una parte constante sobre todo el tratamiento de riesgos como lo expresa la norma NTC-ISO/IEC 27005:

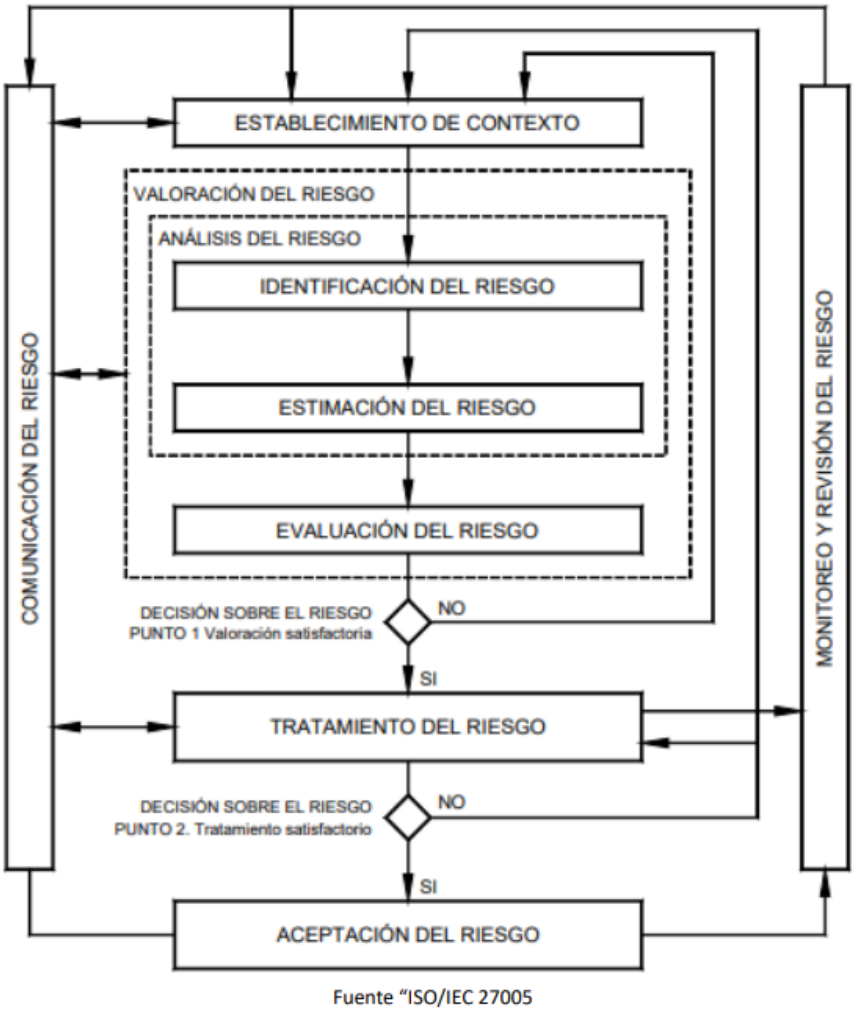

Figura 1 Propuesta la comunicación del riesgo. Fuente ISO/IEC 27005

Durante todo el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia por parte de los directores y el personal acerca de los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información y de los dos puntos de decisión sobre el riesgo.

El Instituto Universitario de la Paz – UNIPAZ dando cumplimiento a los requisitos de norma, diseña el presente plan para operativizar las actividades de implementación y aseguramiento de la ejecución de cada una de sus fases, por lo tanto, el presente plan, está encaminado a identificar dichas actividades que a la fecha se encuentran pendientes por ejecutar y trazar una hoja de ruta que permita avanzar en la implementación de controles para mitigar los riesgos.

A continuación, se presentan la estructura de la metodología de riesgos y actividades que permitirán desarrollar e implementar, lo dispuesto en el presente Plan. La metodología está integrada por las siguientes etapas:

1. Establecer el contexto: Permite a los responsables y/o lideres de procesos describir el entorno y las situaciones particulares de ésta, con los actores del ámbito de su dependencia.

2. Identificar el Riesgo: Establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación y del modelo de gestión, con este punto se revisa la pertinencia del alcance planteado para el MSPI.

3. Evaluación de los riesgos: Los responsables y/o lideres de procesos identifican, analizan y evalúan los riesgos a fin de determinar aquellos que por su impacto y probabilidad de ocurrencia pueden afectar el cumplimiento de las metas y objetivos de su dependencia.

4. Tratamiento de los Riesgos: Son las etapas de identificación y análisis de riesgos, de esta forma se busca escoger los controles que permitan disminuir los valores de exposición, daño o perdida del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad de la Información.

5. Aceptación del Riesgo: Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

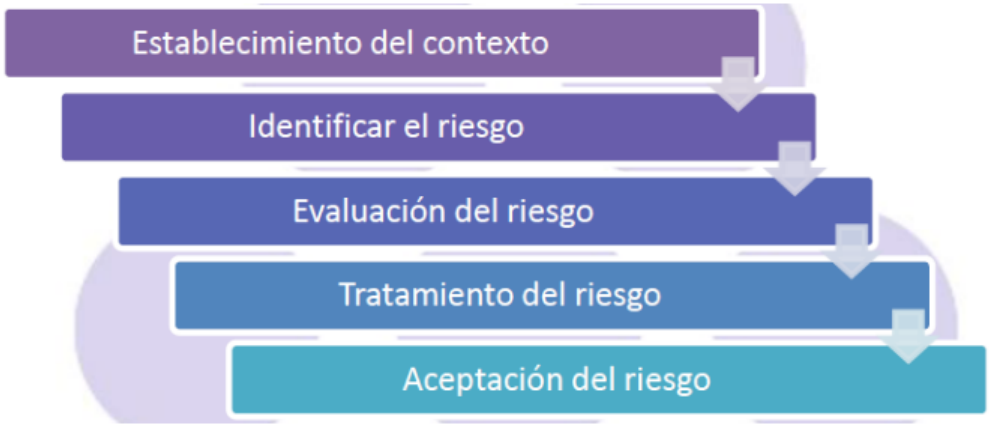

Figura 2 Estructura general de la metodología de riesgo

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

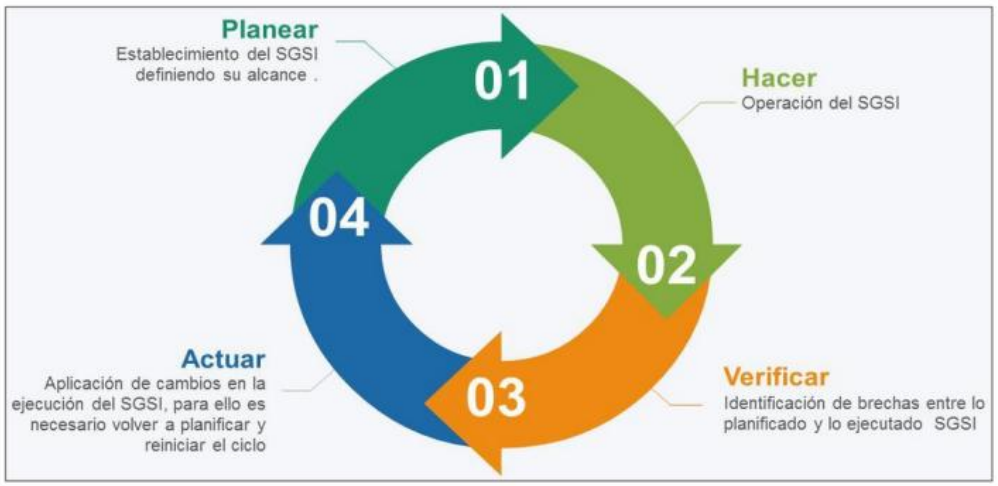

Figura 3 Ciclo PHVA

7. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación y valoración de los riesgos de seguridad de la información está compuesto por los siguientes hitos o actividades:

7.1. Programación y agendamiento de entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del sistema integrado de gestión de la calidad de la institución y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

7.2. Entrevistas con los líderes de procesos

Se entrevista a cada líder de proceso, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

7.3. Identificación y calificación de riesgos

En el proceso de identificar los riesgos, es clave contar con información coherente y actualizada acerca de las actividades que se llevan a cabo en los diferentes procesos, los resultados esperados de las mismas, como orígenes de riesgos, se puede acudir a diversas fuentes de información.

7.4. Valoración del riesgo residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

- Las fuentes de riesgos materiales, las que podemos ver y las fuentes de riesgos que no podemos identificar a simple vista o que existe y se pasan por alto.

- Del análisis de contexto extraer las amenazas y debilidades para la identificación de riesgos y las oportunidades de mejora.

- Caracterizar los activos y recursos con los que cuenta UNIPAZ, identificando su naturaleza, importancia y valor.

- Los aspectos relacionados con los tiempos.

7.5. Mapas de calor donde se ubican los riesgos

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

8. METODOLOGÍA

El Plan de Tratamiento de Riesgos de Seguridad de la Información, contempla la definición de las actividades a desarrollar, en aras de mitigar los riesgos sobre los activos de información, 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 (MinTIC:2016):

Tabla 2 Actividades para la implementación del plan de tratamiento de riesgos

ACTIVIDAD	RESPONSABLE
Adopción Plan de implementación del tratamiento de los riesgos en seguridad digital	Comité CIGDAC - Comité Institucional de Gestión, Desempeño y Aseguramiento de la Calidad
Definición del plan de levantamiento y caracterización de activos de información del Instituto Universitario de la Paz - UNIPAZ	Asesor de Tecnologías de la Información y las Comunicaciones
Levantamiento de los activos de información del Instituto Universitario de la Paz - UNIPAZ	Asesor de Tecnologías de la Información y las Comunicaciones - Todas las dependencias
Formación a los delegados de cada dependencia en la identificación de riesgos de seguridad de la información	Asesor de Tecnologías de la Información y las Comunicaciones
Identificación, análisis y evaluación de riesgos	Asesor de Tecnologías de la Información y las Comunicaciones - Todas las dependencias
Gestión del tratamiento de los riesgos identificados	Comité CIGDAC - Comité Institucional de Gestión, Desempeño y Aseguramiento de la Calidad
Implementación de controles	Asesor de Tecnologías de la Información y las Comunicaciones

9. MONITOREO Y REVISIÓN

El Instituto Universitario de la Paz – UNIPAZ, a través de las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota: Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la institución debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgo. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

9.1. Registro y reporte de incidentes

Es importante que El Instituto Universitario de la Paz – UNIPAZ, cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles. Igualmente, se deben realizar el reporte de incidentes de seguridad de la información a los entes de control, reguladores, superintendencias, y demás autoridades en la materia, conforme lo estipulan los entes o las buenas prácticas establecidas en seguridad digital.

9.2. Reporte de la gestión del riesgo

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

Matriz de los riesgos identificados de seguridad digital.
Listado de activos críticos TI/TO y listado de ICC.
Reporte de criticidad sobre impacto de la organización.
Plan de tratamiento de riesgos.
Reporte de evolución de riesgos y modificación del apetito de riesgo.
Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
Impacto económico que podría presentarse frente a la materialización de los riesgos.

9.3. Reporte de a autoridades o entidades especiales.

Periódicamente por parte de las Entidades u organizaciones
Que han adaptado el modelo respectivo.
Cuando ocurra un cambio organizacional o de los procesos de la organización que genere un impacto en las operaciones o pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de los riesgos y reportar los resultados a la entidad de control.
Cuando se incluya un nuevo proceso dentro del alcance de la gestión de riesgos de seguridad digital de la organización. En este caso se debe realizar una nueva evaluación de riesgos y reportar los resultados a la Entidad de

Una vez el Instituto Universitario de la Paz – UNIPAZ obtenga los resultados de la gestión de riesgos de seguridad digital, se deberá consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad digital.

Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico

- Amenazas críticas
- Vulnerabilidades críticas
- Tipos de activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet)
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad digital de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

- **Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:**

Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deberían reportarse a las autoridades o instancias encargadas.

Nota: Es importante indicar que los reportes de riesgos de seguridad digital a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

9.4. Auditorías internas y externas

Le corresponde a la Oficina de Evaluación y Control (tercera línea de defensa), realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en el Instituto Universitario de la Paz - UNIPAZ, catalogándola como una unidad auditable más dentro de su universo de auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional.

9.5. Medición del desempeño

La institución debe utilizar medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente y alineadas con la revisión por la línea estratégica.

9.5.1. Indicadores - gestión del riesgo de seguridad digital

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados. La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.

- 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

10. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

Una vez se haga la identificación de los riesgos su análisis y establecimiento de controles, se deben establecer líneas de defensa o acciones a seguir, en caso de materialización de cada uno de los riesgos identificados.

Adicionalmente, se debe establecer un procedimiento que permita reevaluar los riesgos para establecer controles que permitan la no materialización de un riesgo futuro.

11. MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

La institución debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse. Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

· Revisar y evaluar los hallazgos encontrados en las auditorías internas realizadas, otras auditorías e informes de los entes de control.

· Establecer las posibles causas y consecuencias del hallazgo.

· Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.

· Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

12. PLAN DE COMUNICACIONES

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 la institución 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.

13. HOJA DE RUTA / PLAN DE ACCIÓN

ACTIVIDAD	RESPONSABLE	2025											
		Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Adopción del Plan de implementación del tratamiento de los riesgos en seguridad digital	Comité CIGDAC - Comité Institucional de Gestión, Desempeño y Aseguramiento de la Calidad												
Definición del plan de levantamiento y caracterización de activos de información del Instituto Universitario de la Paz - UNIPAZ	Asesor de Tecnologías de la Información y las Comunicaciones												
Levantamiento de los activos de información del Instituto Universitario de la Paz - UNIPAZ	Asesor de Tecnologías de la Información y las Comunicaciones - Todas las dependencias												
Formación a los delegados de cada dependencia en la identificación de riesgos de seguridad de la información	Asesor de Tecnologías de la Información y las Comunicaciones												
Identificación, análisis y evaluación de riesgos	Asesor de Tecnologías de la Información y las Comunicaciones - Todas las dependencias												
Gestión del tratamiento de los riesgos identificados	Comité CIGDAC - Comité Institucional de Gestión, Desempeño y												

ACTIVIDAD	RESPONSABLE	2025											
		Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
	Aseguramiento de la Calidad												
Implementación de controles	Asesor de Tecnologías de la Información y las Comunicaciones												