UNIVERSIDAD DEL QUINDÍO
Res.MEN 014915 - 02 AGO 2022
RENOVACIÓN ACREDITACIÓN

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

Oficial de Seguridad y Privacidad de la Información

UNIQUINDÍO
en conexión territorial
www.uniquindio.edu.co

CONTENIDO

INTRODUCCIÓN

La Universidad del Quindío en cumplimiento a lo establecido en el Decreto 612 de 2018 y siendo consciente de los riesgos que se generan con el uso de las tecnologías de la información, define el plan de tratamiento de riesgos de seguridad y privacidad de la información. Lo anterior, de acuerdo al alcance del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, para la vigencia 2023.

La definición del Plan de Tratamiento de Riesgos permite determinar las medidas necesarias para mitigar la probabilidad o el impacto de los riesgos identificados por los líderes de los procesos; minimizando la posibilidad de pérdida de confidencialidad, integridad o disponibilidad de los activos de información; lo que contribuye a la disminución de situaciones que puedan generar inconvenientes para el cumplimiento de los objetivos estratégicos de la Universidad del Quindío.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información soporta los planes específicos definidos en cada proceso para el tratamiento de sus riesgos. En dichos planes se detalla las actividades a desarrollar, los responsables de cada actividad, fechas de ejecución, indicadores y seguimientos.

Las actividades descritas en este plan se definieron teniendo en cuenta: el estado actual frente a la adopción del MSPI en la universidad, el contexto de la institución, las restricciones, la información del análisis de riesgos realizada por cada uno de los procesos del alcance del SGSPI y los objetivos propuestos frente a la gestión de riesgos de seguridad de la información.

1. OBJETIVOS

General

Establecer las fases para la ejecución de los planes de tratamiento de los Riesgos de Seguridad y Privacidad de la Información en la Universidad del Quindío, en cumplimiento de las normativas aplicables a la institución y con el fin de minimizar la ocurrencia de eventos que puedan impactar de manera negativa los objetivos estratégicos, la misión y la visión de la entidad; preservando la integridad, confidencialidad, disponibilidad de la información.

Específicos

- Dar cumplimiento a los lineamientos del Gobierno Nacional y a lo expedido por el Ministerio de Tecnologías de la información y las Comunicaciones (MinTIC) así como el cumplimiento de los requisitos legales y regulatorios pertinentes, relacionados con la seguridad de la información y la privacidad y protección de datos personales.
- Proteger la información que genera, procesa, transmite, gestiona y almacena la universidad; así como garantizar la disponibilidad de los procesos y sus servicios.
- Evaluar las amenazas actuales y futuras de la información, mediante la gestión de riesgos de seguridad de la información.
- Gestionar los riesgos de Seguridad y Privacidad de la información, de acuerdo con el contexto de la institución y el alcance del SGSPI.
- Promover la mejora continua, mediante el proceso de gestión de riesgos de Seguridad de la Información y la evaluación de la eficacia de los planes de tratamiento.
- Fortalecer y apropiar a los líderes de proceso, con el conocimiento requerido para la gestión de riesgos de Seguridad y Privacidad de la información aplicables a su proceso.

2. ALCANCE

Este documento aplica a los procesos del alcance del SGSPI en el marco de la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI y en

concordancia a lo establecido en el Decreto 612 de 2018, la Política de Gobierno Digital y Seguridad Digital, la Norma ISO/IEC 27001 y demás lineamientos gubernamentales relacionados con este tema: para las vigencias de 2023, 2024 y 2025.

3. MARCO NORMATIVO

A continuación, se listan algunas de las normas más relevantes, que dan soporte a la operación del SGSPI. La totalidad de las normas o los soportes legales y reglamentarios están descritos en el normograma del sistema de gestión:

- **La Ley 527 de 1999:** "Por medio de 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 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 usen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- **Ley 1581 de 2012**: "Por la cual se dictan disposiciones generales para la protección de datos personales". Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

- **Norma ISO/IEC 27001:2013**: Sistemas de Gestión de Seguridad de la Información.

- **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". Reglamentada parcialmente por el Decreto Nacional 103 de 2015.

- **Decreto Nacional 2573 de 2014:** "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

- **Decreto 1078 del 26 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- **Documento CONPES 3995 de 2020:** "Política Nacional de confianza y Seguridad Digital".

- **Directiva Presidencial 03 de marzo de 2021:** Por medio de la cual se establecen los "Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de datos."

- **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 2022 (MinTIC):** "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"

4. DEFINICIONES[1]

A continuación, se listan los términos que podrían usarse dentro del documento con su respectiva definición.

- **Activo de información:** Todo aquello que tiene valor para la entidad, por lo tanto, debe protegerse. De acuerdo con la norma ISO/IEC 27001, los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Confidencialidad**: Que la información solo sea accedida por las personas autorizadas para ello.

[1] Definiciones contenidas en la ISO 27000. Extraídas del sitio web: https://www.iso27000.es/glosario.html

- **Control o Medida:** Medida que permite reducir o mitigar un riesgo
- **Impacto**: consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Incidente:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Riesgo**: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales[2].
- **Riesgo de Seguridad de la Información:** 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. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguridad informática:** Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

[2] Algunas de las definiciones fueron tomadas de Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

5. MARCO DE REFERENCIA PARA EL PROCESO

5.1. Política de Administración de Riesgos

La Universidad del Quindío cuenta con la Política de Administración de Riesgos aprobada mediante Resolución No. 7322 del 27/07/2020; la cual describe de una manera integral, entre otros:

- Tipo de Riesgos a tratar
- Normatividad aplicable de acuerdo al tipo de riesgo
- Metodologías a implementar para la administración de los riesgos
- Opciones para el tratamiento
- Responsabilidades de acuerdo a las líneas de defensa
- Técnicas para identificación de oportunidades
- Periodicidad de los monitoreos y revisiones
- Formas de información, comunicación y reporte
- Formas de documentación del proceso

Sumado a lo anterior, para los riesgos de seguridad y privacidad de la información, se cuenta con una Guía Metodológica, donde se describe:

La Universidad del Quindío define como “Moderado” su Nivel de Riesgo Aceptable – NRA para los riesgos de seguridad de la información, por lo tanto, se establecerán planes de respuesta para los riesgos identificados en las zonas “Alto” y “Extremo”.

El proceso de gestión de riesgos de seguridad de la información contiene las siguientes fases:

- Comprensión del contexto.
- Identificación del riesgo de seguridad de la información.
- Análisis del riesgo de seguridad de la información.
- Evaluación del riesgo de seguridad de la información.
- Tratamiento del riesgo de seguridad de la información.
- Comunicación del riesgo de seguridad de la información.
- Monitoreo y revisión del riesgo de seguridad de la información.

En dicho documento se especifica cada una de las fases y se muestra el mapa de calor, escalas de medición y la forma de analizar y evaluar los riesgos; de acuerdo a la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas v5",* de fecha diciembre de 2020 del Departamento Administrativo de la Función Pública – DAFP.

6. DESCRIPCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, 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)[3]

	Actividad	Descripción	Responsable	Fechas de ejecución	
				Inicio	Final
Administración de Riesgos	Actualizar de directrices y/o documentos relacionados con la gestión de riesgos	Apoyar cuando se requiera la actualización de la política, Guía metodológica y demás lineamientos de la gestión de riesgos	Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	01/Feb/2023	30/Nov/2023
	Sensibilizar y/o comunicar	Socializar las directrices y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	01/Mar/2023	30/Mar/2023
	Realizar proceso de identificación, evaluación y análisis de riesgos de seguridad y privacidad de la información	Analizar el contexto, Identificar, Analizar y Evaluar los Riesgos - Seguridad y Privacidad de la Información de acuerdo a la metodología.	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de	01/Mar/2023	30/Mar/2023

[3] Ibidem

			Planeación Institucional		
		Realimentar a las partes interesadas, realizar revisión y verificación de los riesgos identificados y valorados (Ajustes)	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	**01/Mar/2023**	**30/Mar/2023**
	Definir y aceptar los Planes de Tratamiento de Riesgos	Definir los planes de tratamiento de los riesgos que se encuentren por encima del nivel aceptable de los riesgos, de acuerdo a la metodología.	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	**01/Mar/2023**	**30/Mar/2023**
		Aceptar y aprobar los riesgos identificados y sus respectivos planes de tratamiento.	Líderes de proceso del alcance del SGSPI. Comité Institucional de Gestión y Desempeño.	**01/Mar/2023**	**30/Mar/2023**
Administración de Riesgos	Realizar publicación y/o Comunicación	Publicar los riesgos de seguridad y privacidad de la información de los procesos de acuerdo a las directrices definidas por la universidad	Profesional de la Dirección de Planeación Institucional	**01/Mar/2023**	**30/Mar/2023**
	Realizar seguimiento a los Riesgos y Planes de Tratamiento	Realizar seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	**15/Abr/2023**	**30/Nov/2023**
	Mejoramiento	Identificar las oportunidades de mejora De acuerdo al resultado del seguimiento de la implementación de los controles de seguridad y	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y	**15/Abr/2023**	**30/Nov/2023**

		privacidad de la información y de los planes de tratamiento	Privacidad de la Información. Profesional de la Dirección de Planeación Institucional		
Administración de Riesgos		Revisión y/o actualización de los Riesgos de Seguridad y privacidad de la información; así como sus respectivos planes de tratamiento de acuerdo con los resultados obtenidos en los seguimientos, los incidentes de seguridad de la información presentados y/o la materialización de los riesgos; o según las observaciones presentadas por la Dirección de Planeación Institucional.	Líderes de proceso del alcance del SGSPI. Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	**15/Abr/2023**	**30/Nov/2023**
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Oficial de Seguridad y Privacidad de la Información. Profesional de la Dirección de Planeación Institucional	**15/Abr/2023**	**30/Nov/2023**

Tabla 1. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Nota: Los controles seleccionados para los riesgos de Seguridad y Privacidad de la Información serán relacionados con los descritos en el Anexo A de la norma la ISO 27001; a fin de determinar las acciones específicas para el tratamiento e identificar las posibles vulnerabilidades en la Universidad del Quindío, en lo referente a los mismos.

7. MATERIALIZACIÓN DE RIESGOS

Si durante la vigencia se materializar un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información, definido por la universidad, a través del CSU. Así mismo se deberá realizar el proceso de identificación, análisis y valoración del riesgo, para determinar si los niveles de probabilidad e impacto fueron modificados, o si los controles implementados no fueron suficientes o efectivos para el tratamiento de los mismos, después de la materialización. Se registran los cambios en las matrices de riesgo de cada proceso.

En caso de materialización de un riesgo que no esté identificado, éste se deberá documentar y realizar todo el proceso de administración, de acuerdo a la metodología definida para tal fin.

8. RECURSOS PARA LA GESTION DE LOS RIESGOS DE SEGUIRDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los recursos con los que cuenta la universidad para la administración de los riesgos de Seguridad y Privacidad de la Información son:

RECURSOS	DESCRIPCIÓN
Humanos	• Profesional de Planeación Institucional • Oficial de Seguridad y Privacidad de la Información • Líderes de Proceso del alcance del SGSPI • Equipo de Respuesta a Incidentes de Seguridad de la Información (Dirección TI)
Técnicos	• Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP • Política para la Administración de Riesgos • Guía para la Gestión de Riesgos de Seguridad y Privacidad de la Información • Matriz para la Gestión de Riesgos de Seguridad y Privacidad de la Información • Herramienta para el registro, seguimiento y control de Riesgos de Seguridad y Privacidad de la Información (GPSecure)
Logísticos	• Procedimientos para la gestión de recursos para realizar socializaciones, transferencias de conocimiento y seguimiento a la gestión de riesgos y sus planes de tratamiento.
Financieros	Los recursos financieros dependen de las aprobaciones dadas por el Comité Institucional de Gestión y Desempeño, cuando se presentan los planes de tratamiento y se definen los proyectos de inversión para el fortalecimiento de la seguridad de la información (física y/o digital) en la Universidad del Quindío.

Tabla 2. Recursos para la Gestión de Riesgos de Seguridad y Privacidad de la Información

9. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO DE RIESGOS DE SEGUIRDAD Y PRIVACIDAD DE LA INFORMACIÓN

La estimación y asignación del presupuesto para la implementación de los planes de tratamiento de riesgos de Seguridad y Privacidad de la Información, se determinará de acuerdo a las aprobaciones dadas por el Comité Institucional de Gestión y Desempeño y a lo solicitado por los dueños de los riesgos (líderes de los procesos), quienes son los responsables de la implementación y seguimiento de los planes de tratamiento de los riesgos identificados en cada uno de sus procesos.

10. MEDICIÓN, SEGUIMIENTO Y MONITOREO DE LOS RIESGOS Y SUS PLANES DE TRATAMIENTO

La medición, seguimiento y monitoreo de los riesgos de Seguridad y Privacidad de la Información, así como de sus controles y planes de tratamiento, se realiza por parte de la Dirección de Planeación Institucional; teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas en la política y la guía que contiene la metodología. Lo anterior, después de validados los resultados de los seguimientos realizados por los líderes de los procesos en conjunto con el Oficial de Seguridad y Privacidad de la Información, a cada uno de los riesgos identificados en los procesos; así como los soportes que sean requeridos por la Dirección de Planeación Institucional.

La medición, seguimiento y monitoreo de los riesgos y sus planes de tratamiento se realizará a través del indicador " Tratamiento de Riesgos de Seguridad de la Información" definido en el marco de la implementación del SGSPI; dicho indicador tiene como propósito:

1. Determinar cuántos riesgos de los identificados tienen definidos planes de tratamiento; con el fin de determinar la adecuada gestión de riesgos de seguridad de la información en la universidad, de acuerdo a los niveles de aceptación definidos en la metodología

2. Medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la información, cuyo propósito es Identificar el grado de avance en la implementación de controles de seguridad de la información definidos en los planes de tratamiento para mitigar los riesgos identificados por los procesos.

Nombre del Indicador	Tipo de Indicador	Numeral/Anexo A de la norma ISO 27001:2013 asociado	Objetivo del SGSPI asociado	Fórmula	Frecuencia
Tratamiento de Riesgos de Seguridad de la Información	Eficacia	6.1.3. Tratamiento de riesgos de la seguridad de la información	**2**. Gestionar los riesgos de seguridad de la información de acuerdo a la metodología y plan de tratamiento utilizados para mantenerlos en niveles aceptables	(# de riesgos del MSPI de los niveles alto y extremo con planes de tratamiento/ Total riesgos del MSPI definidos en los niveles alto y extremo) * 100	Trimestral
				(# de Controles del plan de tratamiento Implementados / Total de Controles que se planearon implementar) * 100	Trimestral

Tabla 3. Indicadores para la medición de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

11. ANEXOS Y/O COMPLEMENTOS

- Política para la Administración de Riesgos
- Guía para la Gestión de Riesgos de Seguridad y Privacidad de la Información
- Matriz para la Gestión de Riesgos de Seguridad y Privacidad de la Información
- Herramienta para el registro, seguimiento y control de Riesgos de Seguridad y Privacidad de la Información (GPSecure)

DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL

Tel: (57) 6 735 9300 Ext
Carrera 15 Calle 12 Norte
Armenia, Quindío – Colombia
sgsi@uniquindio.edu.co