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

OFICINA DE SISTEMAS
2024

CONTENIDO

INTRODUCCIÓN

La gestión de riesgos de seguridad digital debe considerar la implementación de medidas que implican tiempo, esfuerzos y recursos 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 de la Universidad.

Este plan describe las actividades que se deben llevar a cabo para realizar la identificación, valoración, y tratamiento de los riesgos de seguridad sobre los activos de información de la Universidad, alineado con la política de gestión integral del riesgo, con el fin de preservar la seguridad e integridad de los activos; de acuerdo a lo establecido en la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP.

Estas acciones son organizadas de acuerdo a unas fases, y para cada una de ellas se define la acción, el responsable y la fecha límite de realización.

1. OBJETO

Definir las actividades necesarias para el proceso de identificación de los riesgos de seguridad digital sobre los activos de información de cada uno de los procesos de la Universidad, y evaluación de las posibles acciones para mitigarlos de manera preventiva e integral, contribuyendo así a protección de la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

El alcance del presente plan de tratamiento de riesgo es aplicable a todos los procesos de la Universidad de los Llanos con manejo de activos de información.

3. REFERENCIAS NORMATIVAS

- **Decreto 1078 de 2015.** Por medio del cual se expide el decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones.
- **Decreto 1008 de 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Norma Técnica Colombiana NTC-ISO/IEC 27005** Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas- 2022** - *Versión 6* -DAFP.
- **Acuerdo Superior 012 de 2020,** *"Por el cual se adopta la Política para la Gestión Integral de Riesgos en la Universidad de los Llanos".*
- **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 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.
- **Decreto 767 de 2022.** Actualización Política de Gobierno Digital.

4. DEFINICIONES

- **Activo:** Cualquier recurso de la empresa necesario para desempeñar las actividades diarias. La valoración de los activos es importante para la evaluación de la magnitud del riesgo
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Criterio**: Regla o norma conforme a la cual se establece un juicio o se toma una determinación.
- **Estimación del riesgo**: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Identificación del riesgo**: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Impacto:** Efecto positivo o negativo, resultado y/o consecuencias de la materialización de un riesgo.
- **ISO/IEC 27005**: Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de la información en una empresa.
- **Probabilidad:** Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento.
- **Reducción del riesgo**: Acciones que se toman para disminuir la probabilidad de las consecuencias, sin que suponga un perjuicio demasiado grave en los diferentes niveles institucionales.
- **Riesgo de Corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo Inherente:** Se refiere al riesgo identificado inicialmente sin aplicar ninguna medida de tratamiento.
- **Riesgo residual**: Riesgo que permanece después de la implementación de controles.
- **Riesgo:** Es la probabilidad de que ocurra un evento y una amenaza se materialice causando efectos negativos.
- **Transferencia del riesgo**: Compartir con otras partes la pérdida o la ganancia de un riesgo.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES

No se establecen condiciones generales para este documento.

6. CONTENIDO

6.1. Metodología Gestión de Riesgos

El proceso para la gestión de riesgos de Seguridad Digital en la Universidad de los Llanos, se realizará acorde con la metodología descrita en el procedimiento "*PD-DIE-03 - Gestión de los Riesgos y Oportunidades Institucionales*" en su versión vigente, la cual debe cumplir con lo establecido en la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas"* emitida por el Departamento Administrativo de Función Pública-DAFP y el modelo de gestión de riesgos descrito en el anexo 4 *"Modelo Nacional de Gestión de Riesgo de seguridad de la Información en Entidades Públicas"* en su versión vigente.

6.2. Tratamiento del Riesgo

Como resultado de la etapa de evaluación del riesgo tendremos una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas-DAFP".*

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento.

Para el tratamiento de cada uno de los riesgos analizados y evaluados la Política institucional define las siguientes estrategias para combatir el riesgo:

- **Aceptar**: Se trata de asumir el riesgo y las consecuencias que implican la materialización del mismo. Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.
- **Compartir o transferir**: Trasladar a un tercero ajeno al proceso la gestión del riesgo. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.
- **Evitar**: Cuando los escenarios de riesgo identificado se consideran demasiados extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.
- **Reducir**: Se espera disminuir el impacto de la materialización del riesgo, debilitando los efectos negativos. El nivel de riesgo debe ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

6.3. Cronograma

Los riesgos de seguridad digital identificados se reflejarán en la matriz de riesgos de seguridad digital, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas apoyará el proceso de definición de los controles con los líderes de cada uno de los procesos o dependencias.

Las actividades a ejecutar para lograr la identificación de los riesgos de seguridad digital sobre los activos de información de los diferentes procesos de la Universidad, conforme a los criterios y al apetito de riesgos previamente definidos en la Política de Gestión Integral del Riesgo de la Universidad son las siguientes:

Tabla 1. Cronograma

Fase	Actividades	Responsables	Fecha Inicio	Fecha Final
Identificación de los activos de información	Identificación, clasificación y valoración de activos de información de criticidad alta en cada uno de los procesos	Prof. de seguridad de la información Líderes de procesos	Julio 2024	Diciembre 2024

Fase	Actividades	Responsables	Fecha Inicio	Fecha Final
Identificación y valoración de los riesgos de seguridad de la información	*Identificar las amenazas y las vulnerabilidades a las que se encuentran expuestos los activos de información en cada uno de los procesos. *Identificar los controles existentes. *Identificar consecuencias. *Valorar las consecuencias. *Determinar el nivel de estimación del riesgo. *Evaluar el riesgo.	Prof. de seguridad de la información Líderes de procesos	Julio 2024	Diciembre 2024
Tratamiento de los riesgos	Identificar, valorar y definir las opciones de tratamiento (selección de controles) para los riesgos de seguridad de la información identificados en cada uno de los procesos.	Prof. de seguridad de la información Líderes de procesos	Julio 2024	Diciembre 2024
Monitoreo y Revisión	Realizar monitoreo de los riesgos identificados	Prof. de seguridad de la información Líderes de procesos Oficina de Control Interno	Abril 2025	Diciembre 2025
Mejoramiento Continuo	Analizar la eficacia del tratamiento de los riesgos y determinar acciones de mejora en caso de que sean necesarias	Líder proceso Gestión TIC Profesional de seguridad de la información	Abril 2025	Diciembre 2025

Fuente: Elaboración propia.

6.4. Recursos

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que se requieran para el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección.

7. FLUJOGRAMA

No aplica.

8. LISTADO DE ANEXOS:

El documento no tiene anexos.

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
01	15/12/2021	Documento nuevo.	Andrea Pinilla *Prof. Apoyo Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*
02	27/09/2022	Se reestructuró el documento y sus actividades.	Mónica Hernández *Prof. Seguridad de la Información*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*
03	04/07/2024	Se actualizó el documento para la vigencia 2024.	Mónica Hernández *Prof. Seguridad de la Información*	*Roiman A. Sastoque* *Jefe Oficina de Sistemas*	*Roiman A. Sastoque* *Jefe Oficina de Sistemas*