UNP

Informe de Monitoreo de Segunda Línea de Defensa – Gestión de Riesgos de Seguridad de la Información UNP III Cuatrimestre 2024

Oficina Asesora de Planeación e Información
Unidad Nacional de Protección
15-11-2024

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVO GENERAL 3
3. METODOLOGÍA 3
3.1 Monitoreo de controles 4
4. CONTEXTO GENERAL 4
4.1 Análisis de distribución de Riesgos 4
4.2 Causas o Eventos Potenciales Comunes Identificadas en Los Procesos 6
4.3 Análisis de Vulnerabilidades 6
5. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS 7
6. RECOMENDACIONES 9
7. ANEXOS 10

1. INTRODUCCIÓN

La administración de riesgos es un proceso coordinado y preventivo que tiene por objeto el aseguramiento del logro de los objetivos institucionales y de los procesos de la Entidad, en el marco de la adopción e implementación del Modelo Integrado de Planeación y Gestión MIPG y de la implementación de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad de la Información Digital y del Diseño de Controles en Entidades Públicas versión 6 de 2022.

La UNP desarrolla este proceso con la revisión y formulación de la política de Administración de Riesgos Institucionales, la cual establece la actuación de todos los responsables de procesos, coordinadores de Grupos Internos de Trabajo, enlaces MIPG-SIG y demás colaboradores que participan en la operación de los procesos y actividades de la Entidad ejerciendo el rol de Primera línea de Defensa.

Este informe se presenta en cumplimiento del ***Componente 1 - Gestión de Riesgos de Corrupción - Mapa de Riesgos de Corrupción del Subcomponente 3. Consulta y divulgación y Subcomponente 4. Monitoreo y Revisión*** del Plan Anticorrupción y Atención al Ciudadano y en lo contentivo en la Política Integral de Administración de Riesgos en la cual la Alta Dirección de la UNP se compromete a mantener niveles aceptables en los riesgos de todos sus procesos y a promover una cultura institucional basada en la gestión integral del riesgo; mediante la identificación e implementación oportuna de acciones preventivas y de control, orientadas a mitigar, corregir y evitar la materialización de los riesgos institucionales.

El presente informe contiene el análisis de las amenazas, vulnerabilidades y los resultados de la identificación, valoración y tratamiento de los riesgos de seguridad de la información, de los procesos de la UNP con base en el documento GTE-GU-04 Guía de Identificación Valoración y Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2. OBJETIVO GENERAL

Presentar el estado actual de la gestión de riesgos de seguridad de la información en la Unidad Nacional de Protección, correspondiente al segundo cuatrimestre del 2024

3. METODOLOGÍA

Con el fin de identificar las amenazas, vulnerabilidades, análisis de impacto e identificación de controles para mitigar los riesgos de Seguridad de la Información la Oficina Asesora de Planeación e Información (OAPI), realizó acompañamiento a los procesos a través de mesas de trabajo y se identificaron los activos de información como: personas, software, infraestructura, información, hardware, servicios y bases de datos, en los procesos establecidos en el alcance del proyecto Sistema de Gestión de Seguridad de la Información (SGSI) complementado con la metodología descrita en el procedimiento para el proceso de inventario, clasificación y etiquetado de activos de información, de otra parte

se identificaron los riesgos, amenazas, vulnerabilidades relacionadas a los activos de información de la UNP, y poder realizar la identificación y la evaluación los controles implementados para la gestión de los riesgos de acuerdo a la "Metodología de análisis, evaluación y tratamiento de riesgos

De otra parte, al cierre de cada vigencia se invita a los procesos en un ejercicio participativo a supervisar la implementación de prácticas de gestión de riesgo eficaces; apoyando la identificación, análisis, evaluación y tratamiento de los riesgos para la toma de decisiones y acciones preventivas necesarias para evitar su materialización.

A partir del anterior ejercicio, se actualiza el Mapa de Riesgos Institucional que se somete previamente a consulta de la ciudadanía y aprobación interna por parte de los lideres de proceso y se realiza su posterior publicación en la página web de la Entidad.

3.1 Monitoreo de controles

De acuerdo con la identificación de riesgos y definición de controles, la Oficina Asesora de Planeación e Información valida durante el ejercicio de monitoreo en cada cuatrimestre si los controles están implementados y documentados.

4. CONTEXTO GENERAL

La Oficina Asesora de Planeación e Información a través del Grupo de Gestión Integrada y Mejora, según la Política Integral de Administración del Riesgo y el Manual Integral de Gestión de Riesgos, realiza la evaluación del riesgo inherente y del riesgo residual antes y después de la identificación de controles por parte de cada uno de los procesos, con el fin de determinar la administración del riesgo y establecer el plan de tratamiento de riesgos en caso de que se requiera y de esta forma determinar el estado de madurez frente a las buenas prácticas establecidas en la norma para el cumplimiento de la ISO/IEC 27001.

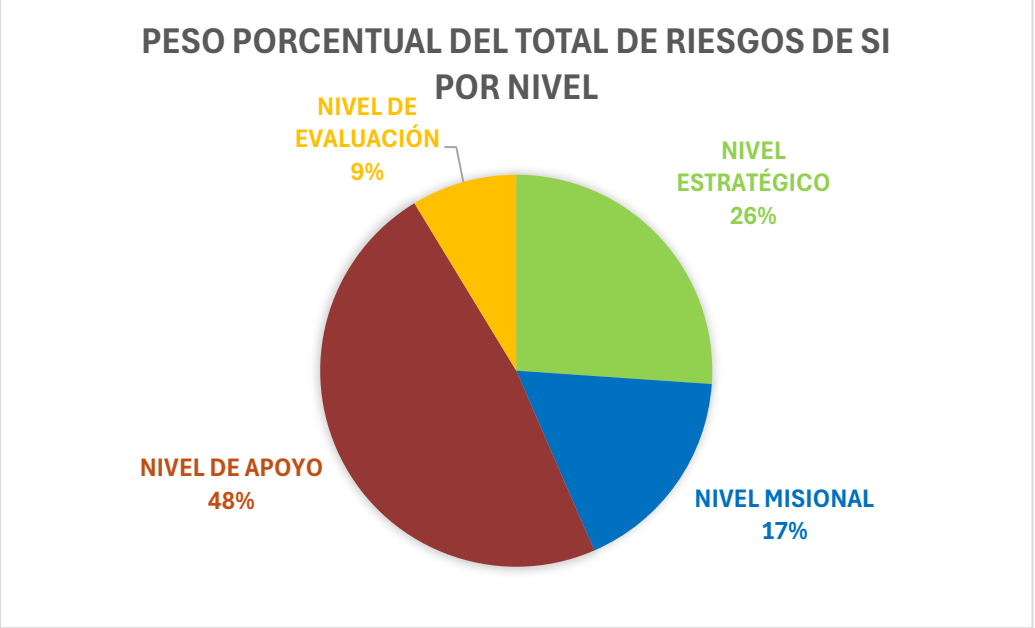
Producto de la revisión se consolidan los resultados a partir de una valoración cuantitativa del presente monitoreo correspondiente al cálculo porcentual de los controles implementados, documentados, así mismo se presenta el avance de las acciones programadas respecto a las implementadas para la vigencia 2024.

4.1 Análisis de distribución de Riesgos

De acuerdo con la matriz de riesgos la UNP cuenta en sus diferentes procesos con un total de riesgos de seguridad de la información identificados en los 18 procesos de cómo se observa en la siguiente tabla:

Tabla No 1 distribución de Riesgos UNP - 2024

NIVEL DE PROCESO	NOMBRE DE PROCESO	TOTAL, RIESGOS
NIVEL ESTRATÉGICO	DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN	1
	GESTIÓN INTEGRADA MIPG-SIG	1
	GESTIÓN ESTRATÉGICA DE TALENTO HUMANO	7
	GESTIÓN DE LAS COMUNICACIONES ESTRATÉGICAS	1
	COOPERACIÓN Y COORDINACIÓN INTERINSTITUCIONAL	2
NIVEL MISIONAL	GESTIÓN INTEGRAL DE MEDIDAS DE EMERGENCIAS	2
	GESTIÓN DE EVALUACIÓN DEL RIESGO	2
	GESTIÓN DE MEDIDAS DE PROTECCIÓN	3
	GESTIÓN ESPECIALIZADA DE SEGURIDAD Y PROTECCIÓN	1
NIVEL DE APOYO	GESTIÓN DE SERVICIO AL CIUDADANO	1
	GESTIÓN DOCUMENTAL	1
	GESTIÓN JURÍDICA	1
	GESTIÓN CONTRACTUAL	1
	GESTIÓN FINANCIERA	2
	GESTIÓN TECNOLÓGICA	6
	GESTIÓN ADMINISTRACIÓN DE Bs Y Ss.	10
NIVEL DE EVALUACIÓN	GESTIÓN EVALUACIÓN INDEPENDIENTE	1
	GESTIÓN CONTROL DISCIPLINARIO INTERNO	3
Total		**46**



4.2 Causas o Eventos Potenciales Comunes Identificados en los Procesos

En los 18 riesgos identificados en los procesos, se analizaron las siguientes causas o eventos potenciales las cuales pueden ser accidentales, ocasionadas propiamente por los procesos o fallas tecnológicas y con base a su resultado, puede presentar daños o pérdidas o interrupciones en los servicios por tanto es importante su evaluación y tratamiento y podrían resultar en afectaciones significativas a la confidencialidad, integridad y disponibilidad de la información de la Entidad.

Una vez identificados los controles y tratamiento de riesgos las causas o eventos más comunes presentados son:

- (Proceso) Implementación de soluciones tecnológicas sin la validación y autorización de gestión tecnológica
- (Proceso) Inadecuado manejo de la información causada por una indebida manipulación de los custodios.
- (Proceso) Falta de conciencia y capacitación en seguridad de la información, que comprometan la confidencialidad, integridad o disponibilidad de la información.
- (Proceso) Ausencia de personal
- (Proceso) Desconocimiento de los lineamientos del SGSI (políticas, normas y procedimientos).
- (Proceso) Desconocimiento y/o incumplimiento de las políticas de Seguridad y Privacidad de la Información
- (Tecnología) Copia no autorizada de información
- (Tecnología) Destrucción de equipos o medios
- (Tecnología) Falta de uso y apropiación en cultura organizacional en Seguridad y Privacidad de la Información
- (Tecnología) Modificación no autorizada de información
- (Tecnología) Uso no autorizado de equipos, falta de conciencia en Seguridad y Privacidad de la Información

De acuerdo con el listado anterior, los procesos deben reunir esfuerzos con el fin de diseñar controles propios y en apoyo con los controles operativos en cumplimiento de las políticas específicas de seguridad de la información y atacar estas posibles causas o eventos potenciales que permitan reducir o mitigar los niveles de riesgos residuales y la materialización de riesgos causando daños o impactos potenciales que podrían afectar la confidencialidad, integridad y disponibilidad de la información de la entidad.

4.3 Análisis de Vulnerabilidades

Las vulnerabilidades son debilidades internas “que son explotadas por amenazas con el objetivo de poner en peligro los activos principales (procesos e información)”, contrario a esto las amenazas son factores y variables que, controladas por la Entidad, se puedan definir acciones y realizar evaluaciones periódicas de los controles definidos. Es por esto por lo que resulta importante definir controles para la mitigación de las vulnerabilidades

técnicas que pueden ser obtenidas por una amenaza, como el hacking malintencionado y materializar riesgos como intrusiones, accesos no autorizados, modificación de información o configuración, que puedan afectar tanto la seguridad de la información como la continuidad del negocio de la Entidad.

4.3.1 Identificación de vulnerabilidades

Según las Amenazas con mayor porcentaje de impacto para la Seguridad de la Información, luego de haber realizado una prueba de vulnerabilidad en los endpoints protection de la UNP para el sistema SOADOC, se evidenció lo siguiente:

1. Apache Solr expuesto en el host 20.62.113.96/solr, con un panel de administración accesible públicamente en una versión obsoleta (6.6.5), lo que permite una posible explotación mediante la ejecución remota de código (CVE-2019-0192).
2. Alfresco Community Edition accesible en el dominio soadoc.unp.gov.co/share/, con una configuración por defecto y credenciales conocidas, lo que expone carpetas internas con información confidencial crítica para la seguridad de la organización.

Esta vulnerabilidad pone en riesgo la confidencialidad, integridad y disponibilidad de los datos gestionados por la UNP, comprometiendo tanto la información protegida como las operaciones críticas de la entidad. Se recomienda implementar medidas de mitigación urgentes para evitar el aprovechamiento de estas vulnerabilidades por actores maliciosos, y fortalecer la seguridad de la infraestructura a través de actualizaciones inmediatas y la limitación del acceso público.

4.3.2 Acciones de mitigación de vulnerabilidades

La subsanación de esta vulnerabilidad se encuentra anexo en carpeta de monitoreo donde se evidencia la gestión realizada y el plan de acción implementado, el cual se documenta a continuación:

1. Actualizar Apache Solr a la versión 7.0 o superior, que incluye parches de seguridad que corrigen esta vulnerabilidad.
2. Acceder a la página de administración de Alfresco y cambiar las credenciales por defecto (usuario/contraseña). Utilizar contraseñas seguras, complejas, y únicas para el administrador y otros usuarios con permisos elevados.

5. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS

Para la evaluación de riesgos, la UNP tuvo en cuenta las vulnerabilidades y amenazas arriba relacionadas y que afectan la Seguridad de la Información de la Entidad, por lo tanto, los resultados están orientados a la mitigación de los riesgos. La respectiva identificación y valoración se realizó con la “Metodología de análisis, evaluación y tratamiento de riesgos”.

El riesgo Inherente y Riesgo Residual se clasifica en las siguientes zonas:

Zona Baja	**B**	**Zona Alta**	**A**
Zona Moderada	**M**	**Zona Extrema**	**E**

5.1 Análisis general para la mitigación de los riesgos en Gestión de Seguridad de la información

Tabla No 2 Análisis de nivel de Riesgos Inherente UNP – 2024

Nivel de Riesgo Inherente	Total, de Riesgos	Peso
Extremo	9	20%
Alto	21	46%
Moderado	15	33%
Bajo	1	2%

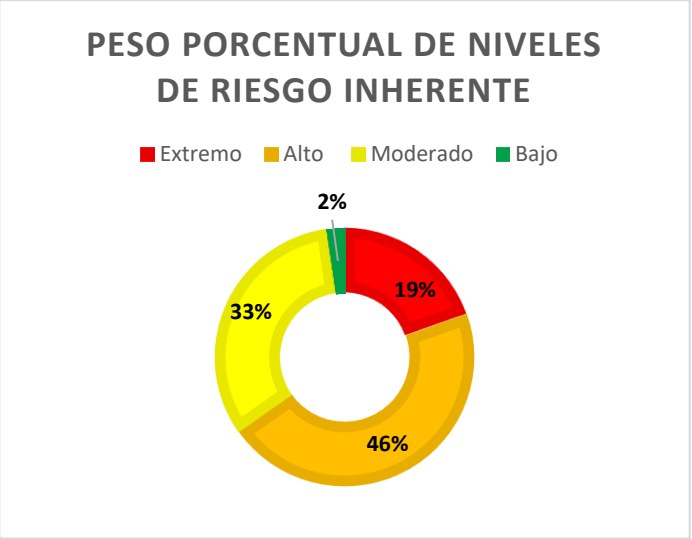
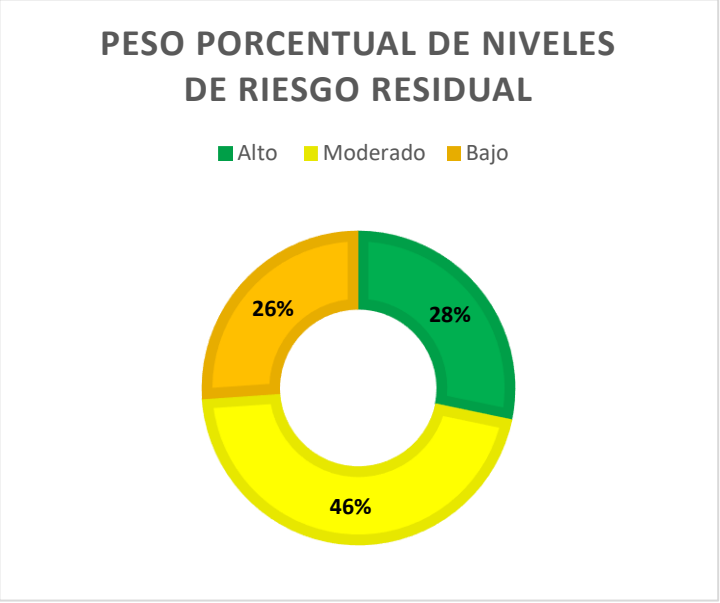


Tabla No 3 Análisis de nivel de Riesgos Residual UNP – 2024

Nivel de Riesgo Residual	Total, de Riesgos	Peso
Alto	13	28%
Moderado	21	46%
Bajo	12	26%



Terminado el ejercicio de monitoreo, se concluye en la tabla anterior el cambio que presentan los riesgos en la zona de calor; de acuerdo con los controles establecidos que mitigan las causas que dan origen al riesgo (disminución de impacto y/o probabilidad); mostrando un desplazamiento importante de los riesgos inherentes, ubicándose residualmente el 28% en la zona alta, el 46% en zona moderada y el 26% en zona baja, en este sentido, las opciones de tratamiento que se deben elegir para tratar los riesgos pueden ser aceptar (Únicamente se permiten para riesgos en nivel de zona residual baja), evitar, mitigar el riesgo.

De otra parte, es importante resaltar que, luego de implementar las actividades de control asociadas a los riesgos identificados, no existen niveles de riesgos extremos, lo cual nos indica que su tratamiento esta diseñado de forma eficaz lo que reduce la probabilidad de ocurrencia e impacto en caso de que se materialicen. Razón por la cual, se deben priorizar el 28% de los riesgos (13 riesgos) que se encuentran en zona de riesgo alta. En este sentido, en la etapa de evaluación de eficacia de controles, la oficina de control interno en su rol de tercera línea de defensa debe enfocar todos los esfuerzos a estos riesgos y evidenciar el cumplimiento del plan de tratamientos de riesgos definidos para cada uno de ellos.

6. RECOMENDACIONES

La OAPI en su rol de Segunda línea de defensa asiste y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, a través del establecimiento de directrices y apoyo a los procesos para identificar, analizar, evaluar y tratar los riesgos y realizar un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

A continuación, se presentan las recomendaciones como producto del monitoreo realizado.

- Orientar esfuerzos en el análisis de los (46) riesgos que se encuentran en zona de riesgo residual alto, y establecer si es necesario medidas de tratamiento especial (disminuir probabilidad y/o impacto), dado que pueden afectar el logro de los objetivos del proceso, planes, programas o proyectos asociados.

- Realizar por parte de la Oficina de Control Interno el seguimiento y evaluación de la eficacia y efectividad de los controles establecidos.

- Promover en el Comité Institucional de Coordinación de Control Interno, el mejoramiento en el tratamiento de los riesgos que pudieron materializarse.

- De acuerdo con la valoración del riesgo residual, efectuar el seguimiento de los riesgos según los lineamientos establecidos en la Política Integral de Administración de Riesgos de la Entidad.

- Continuar fortaleciendo la cultura de gestión de riesgos de seguridad de la información en la UNP.

- Definir las acciones, responsables y fechas de ejecución de los planes de tratamiento de riesgos que están fuera del apetito de riesgo, es importante hacer seguimiento periódico para evaluar el avance de las actividades para dar cumplimiento a los planes y de esta forma gestionar y disminuir el nivel de los riesgos altos, promoviendo el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

7. ANEXOS

La ruta de acceso a los 18 Mapas integrales de Riesgos (MIR), así mismo como la trazabilidad y consolidación de gráficas y la evidencia (Anexo 1) de subsanación de vulnerabilidad identificada en pruebas descrito en informe de gestión, se encuentran en el siguiente link:

Informe de monitoreo de riesgos de SI III cuatrimestre 2024

Firmado digitalmente por JAVIER FRANCISCO RODRIGUEZ MORENO
Fecha: 2024.11.15 16:59:36 -05'00'

JAVIER FRANCISCO RODRÍGUEZ MORENO
Jefe de Oficina Asesora de Planeación e Información (E)

	Nombre	firma	Fecha
Proyectó	Victor Eduardo Benitorevollo Canabal		**15/11/2024**
Revisó	Eliana Elisabeth Mateus Fuente		
Aprobó	Javier Francisco Rodríguez Moreno		
Los arribas firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad, lo presentamos para firma.			