

OFICINA DE CONTROL INTERNO
INFORME SEGUIMIENTO MAPA DE RIESGOS
PROCESO DE GESTIÓN DE SISTEMAS INFORMÁTICOS
VIGENCIA 2019

INTRODUCCIÓN

En atención a lo dispuesto en la Ley 87 de 1993, al artículo 73 de la Ley 1474 de 2011, artículo 3° del Decreto 1537 de 2001, el cual señala: *“El rol que deben desempeñar las Oficinas de Control Interno, dentro de las organizaciones públicas, se enmarca en cinco tópicos a saber: **valoración de riesgos**, acompañamiento y asesoría...”* y el Decreto 648 de 2017 Artículo 2.2.21.5.3 De las Oficinas de Control Interno, indica: *“Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, **evaluación de la gestión del riesgo**,...”*.

La Oficina de Control Interno de la Universidad Pedagógica Nacional, realizó seguimiento y evaluación a los riesgos de gestión por proceso, de conformidad con los lineamientos establecidos en el procedimiento Formulación y Actualización de Mapas de Riesgos PRO009GDC, en la Guía para la Formulación de Mapas de Riesgos GUI002GDC.

OBJETIVO

Realizar seguimiento a las acciones establecidas en el Mapa de Riesgos y valorar si los controles definidos para cada riesgo son efectivos, con el propósito de contribuir a que los riesgos no se materialicen afectando de manera negativa el cumplimiento de los objetivos del proceso e institucionales.

NORMATIVIDAD

- Ley 87 de 1993 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones”.
- 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”.
- Decreto 648 de 2017 “Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentaria Único del Sector de la Función Pública”.
- Guía para la Formulación de Mapas de Riesgos GUI002GDC.
- Procedimiento Formulación y Actualización de Mapas de Riesgos PRO009GDC

RESULTADOS DEL SEGUIMIENTO A LOS RIESGOS IDENTIFICADOS

Código, Riesgo y Zona de Riesgo	Acción de Control y Fecha de Implementación	Evaluación
RIESGOS DE GESTIÓN		
<p>GSI_R37 Deterioro progresivo de la Infraestructura Tecnológica de Hardware, Alta.</p>	<p>Gestión, ejecución y seguimiento a los planes de mantenimiento de la infraestructura tecnológica de Hardware.</p>	<p>Se evidenció, que la Subdirección de Gestión de Sistemas de Información, realiza seguimiento a los planes de mantenimiento tanto de computadores como del Data Center.</p> <p>En cuanto al mantenimiento de computadores, este se realiza de forma directa por la SGSI, por medio de la mesa de ayuda, conforme a los planes de mantenimiento suministrados; adicional entregaron 12 reportes de mantenimiento preventivo de los equipos de cómputo, elaborados a la SAE; es de aclarar que estos mantenimientos, correspondían al cronograma del mes de agosto, sin embargo por necesidad se tuvieron que adelantar.</p> <p>Se sugiere, complementar el diligenciamiento de los formatos de mantenimientos de computadores, y efectuar la publicación de los planes y el cronograma de mantenimientos, a través del mini sitio de la Subdirección.</p> <p>Para el Data center, este se realiza a través del proveedor Cotelgesa; lo que se evidencia con informes del respectivo mantenimiento, entregados por la SGSI.</p>



<p>GSI_R38 Vulnerabilidades de la Seguridad Informática, Alta.</p>	<p>Realización de planes de Mantenimientos e Implementación y ajustes de políticas de seguridad.</p>	<p>La Subdirección de Gestión de Sistemas de información, suministró como evidencia, los mantenimientos efectuados por el proveedor Soft Security, mediante los contratos 855 y 709 de 2018; conforme se ve en los informes de mantenimientos de Antivirus, Hardware y Bases de datos, correspondiente al mes de mayo.</p> <p>Se sugiere unificar la periodicidad de los mantenimientos con la nueva contratación, con el proveedor</p> <p>En cuanto a las políticas de seguridad, con respecto al Data center las dejo implementadas el proveedor y lo relacionado con las Políticas Generales de Seguridad Informática se está trabajando en el tema, el último registro que posee la Subdirección es el envío a la Oficina Jurídica, para la revisión de los últimos ajustes efectuados por el área, esto con fechas 19 de noviembre de 2018 y 9 de julio de 2019.</p> <p>De la misma forma, es procedente efectuar un seguimiento frecuente para dar la celeridad a la liberación, publicación y socialización de las Políticas de seguridad Informática.</p>
<p>GSI_R39 Fallas y Desactualización de los Sistemas de Información. Alta</p>	<p>Gestión, ejecución y seguimiento a los requerimientos de Usuarios y soporte de los Sistemas de Información.</p>	<p>Se evidenció que la Subdirección de Gestión de Sistemas de Información utiliza el aplicativo GLPI, por medio del cual recepciona, gestiona, soluciona o escala los diferentes requerimientos de las dependencias de la UPN.</p> <p>Adicionalmente aportó una base de datos que contienen</p>

		listado de los proveedores activos, con sus respectivos contratos, y cuyo objeto es dar soporte a los sistemas de información de UPN.
--	--	---------------------------------------------------------------------------------------------------------------------------------------

CONCLUSIONES Y RECOMENDACIONES

El área suministró la información de forma completa y dentro de los tiempos establecidos con el fin de reunir los soportes para la verificación de la ejecución de las acciones.

Se observó que la Subdirección viene ejecutando las acciones formuladas, contribuyendo a la eficacia de los controles y por consiguiente aportando al logro de los objetivos del proceso.

Es conveniente que la Subdirección de Sistemas de Información, efectúe un seguimiento permanente, a fin de dar celeridad a la aprobación, publicación y socialización de la Política de Seguridad de la Información, como elemento fundamental para la administración de riesgos del proceso.

Para el riesgo GSI-R37 - Deterioro progresivo de la Infraestructura Tecnológica de Hardware, se recomienda diligenciar los formatos de mantenimiento preventivo de equipos de cómputo; en lo que tiene ver con el cronograma de mantenimiento de computadores, este se debe complementar con información correspondiente a la fecha de elaboración, responsable del mismo y periodicidad, así como efectuar las respectivas publicaciones en el mini sitio de la Subdirección.

Fecha elaboración: 8 de julio de 2019

Firma:


ARELYS VALENCIA VALENCIA
Jefe Oficina de Control Interno

Elaboró: Jenny Vélez