MEMORANDO
No.20191100182843

FECHA: 22/07/2019

PARA: **FERNANDO MARTÍNEZ BRAVO**
Superintendente de Vigilancia y Seguridad Privada
EDGAR RICARDO LOMBO BASTIAS
Secretario General (E)
CLAUDIA MARCELA LADINO HERRERA
Jefe Oficina Informática y Sistemas
OLGA LUCÍA MONJE ÁLVAREZ
Jefe Oficina Asesora de Planeación

DE: **SANDRA MILENA NEIRA SANCHEZ**
Jefe de Oficina de Control Interno

ASUNTO: Informe de Seguimiento a Riesgos en materia de Seguridad de la Información, Contratación y Seguridad y Salud en el Trabajo.

Respetados doctores,

De manera atenta remito para su información y trámite el Informe de Seguimiento en materia de Riesgos de Seguridad de la Información, Contratación y Seguridad y Salud en el Trabajo con corte a junio 30 de 2019. Lo anterior, en cumplimiento del rol de Evaluación de Riesgos a cargo de esta Oficina, establecido en el Decreto 648 de 2017.

Atentamente,

Firmado digitalmente: SANDRA NEIRA SANCHEZ

JEFE DE OFICINA CODIGO 1 4 GRADO 16

Anexo: Lo anunciado en tres (3) folios.

FUNCIONARIO O ANALISTA	NOMBRE
Tramitado y Proyectado por	OMAR URREA ROMERO/NATHALIA ANDREA PINEDA CAMELO
Revisado para firma por	
Los arriba 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 la firma.	

INFORME DE SEGUIMIENTO A RIESGOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN, CONTRATACIÓN Y SEGURIDAD Y SALUD EN EL TRABAJO.

OBJETIVO

Presentar el resultado del seguimiento realizado a los riesgos definidos por la Superintendencia para la vigencia 2019 en los siguientes temas: 1) Seguridad de la Información, 2) Contratación y, 3) Seguridad y Salud en el trabajo. Lo anterior, de acuerdo con los datos tomados del aplicativo SUITE, así como la revisión de documentos y soportes existentes para cada una de las fuentes de riesgo señaladas.

ALCANCE

Se ha analizado la información en materia de estos riesgos, desde enero 01 de 2019 hasta el 30 de junio de la misma vigencia.

METODOLOGIA

Este informe se obtuvo a partir de la aplicación de las siguientes técnicas de análisis:

- Revisión de los reportes de seguimiento a riesgos de la Suite Visión Empresarial con corte a junio 30 de 2019.
- Revisión del Informe de Análisis de la Situación Actual en materia de Riesgos de Seguridad de la Información elaborado por la Empresa MNEMO con corte a diciembre 31 de 2018.
- Revisión de la matriz de riesgos previsibles en materia de contratación prevista por la Superintendencia para sus procesos de contratación.
- Revisión de la matriz de riesgos vigente en la Entidad para el Sistema de Seguridad y Salud en el trabajo.
- Análisis y comparación de la información señalada contra las disposiciones normativas que aplican en materia de riesgos para cada caso: Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública, Requisitos y controles definidos en la norma ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, así como la Guía de Riesgos de la Agencia Nacional de Contratación para el caso específico de los procesos de contratación.
- Preparación de un informe con los resultados del análisis realizado y propuesta de mejora a los riesgos definidos para cada uno de los temas señalados.

RESULTADOS

A continuación, se resumen las principales situaciones evidenciadas como producto del análisis realizado, agrupadas en tres temas: Riesgos en Seguridad de la Información, Riesgos en Contratación y Riesgos en Seguridad y Salud en el Trabajo.

1) RIESGOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

El proceso de Gestión Tecnológica y de Información cuenta con cinco (5) riesgos identificados en el Mapa de Riesgos Institucional para la vigencia 2019. Los mencionados riesgos son los siguientes:

a) No contar adecuadamente con la trazabilidad de los expedientes (integridad, disponibilidad y confidencialidad)

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Omar Urrea Romero
Revisado para firma por	Sandra Milena Neira Sánchez
Los arriba 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 la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

b) No contar con un sistema unificado y válido para consulta de los servicios autorizados actuales en la entidad.

c) No disponer de la información confiable y oportuna que sea de carácter público (Disponibilidad)

d) No disponibilidad y/o fallas en los servicios y en la plataforma de Tecnologías de la información ofrecidos en la entidad.

e) Recibir dádivas para manejo de información (integridad, disponibilidad y confidencialidad)

Para cada uno de los riesgos identificados se definieron acciones para ser ejecutadas durante la vigencia 2019, las cuales se han ido realizando según se evidencia en los reportes de la Suite Visión Empresarial.

Cabe destacar que uno de los controles definidos para el riesgo c), referente a no disponer de la información confiable y oportuna que sea de carácter público consiste en *"Verificación del cumplimiento de los requisitos de la normatividad de Gobierno Digital",* cuyo entregable concreto es un *"Matriz de Gobierno de Digital - actualización de componentes"*, que debe reportarse con corte a junio 30 de 2019. A la fecha, todavía no se evidencia el reporte de esta actividad en la Suite Visión Empresarial.

Entre los riesgos identificados para el proceso no se tienen riesgos específicos en materia de Seguridad de la Información, por lo que éstos se han venido revisando en la Entidad desde otros frentes de trabajo, como es el caso de la contratación en 2018 de una consultoría para la identificación, evaluación y análisis de riesgos, activos de información y análisis de vulnerabilidades de seguridad de la información (Contrato 537 de 2018 con Globaltek Security S.A.S.). Este trabajo incluyó no sólo la identificación de riesgos en materia de seguridad de la información, sino también la identificación de controles y de análisis de vulnerabilidades.

Respecto a los productos concretos de esta consultoría, se recomienda a la Superintendencia incluirlos dentro del Plan de Acción de implementación para el cumplimiento de la norma de seguridad de la información (ISO 27001) y los lineamientos del gobierno nacional en materia de gobierno digital. Lo anterior, resulta particularmente importante para el caso de las Actividades Específicas del Plan de Tratamiento de Riesgos propuesto por la empresa de consultoría en el anexo denominado *"P6-SVSP-Propuesta de controles a implementar"*

De otro lado, a través del Contrato 531 de 2018 con la Empresa MNEMO Colombia SAS, la Superintendencia realizó una pre-auditoría para determinar el nivel de cumplimiento respecto a la norma ISO 27001 en su versión 2013 y los lineamientos definidos por el Modelo de Seguridad y Privacidad de la información del Ministerio de las TICS, establecidos en el marco de los lineamientos del Gobierno Digital.

A modo de ejemplo, en esta pre-auditoría la empresa contratada realizó una revisión de los requisitos de la norma ISO 27001:2013, así como de los 114 controles del anexo A de la norma, con el fin de establecer el nivel de cumplimiento con respecto al Sistema de Gestión de Seguridad de la Información en la entidad. Se produjo el informe respectivo, con el cual la Entidad puede establecer un plan de acción apropiado para ajustarse a los requerimientos de la mencionada norma.

En el informe de pre-auditoría señalado, la empresa contratista señala: *"Si bien es cierto se cuentan con un manual de política de seguridad de la información en la entidad, no se cuenta con la totalidad de los documentos requeridos para la definición del Sistema de Gestión de Seguridad de la Información. Así mismo, no se evidencia actividades asociadas con el análisis y gestión de riesgos de seguridad de la información, inventario de activos de información, métricas e indicadores. Al año 2018, se debería tener implementado, evaluado y con evidencias del mejoramiento continuo del sistema, sin embargo, a la fecha sólo se ha definido algunas de las políticas requeridas por la norma ISO 27001:2013, siendo necesario el desarrollo de las actividades con el fin de mejorar el*

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Omar Urrea Romero
Revisado para firma por	Sandra Milena Neira Sánchez
Los arriba 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 la firma.	

nivel de cumplimiento de los requisitos planteados por el Modelo de Seguridad y Privacidad de la Información" (Página 11 del informe)

A continuación, el informe señalado indica: *"Dentro de los niveles de cumplimiento con respecto al ciclo PHVA, se encuentra que el nivel de Planeación está en un 17% de cumplimiento, el ciclo de Implementación 2%, Evaluación de Desempeño se encuentra en un 3% y el ciclo de Mejora Continua en un 2%. Teniendo en cuenta lo anterior, es importante realizar un esfuerzo significativo, con el fin de lograr cumplir con los requerimientos de la norma ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información, respecto a que se debería estar en proceso de mejora continua del sistema"*

Lo señalado es similar frente al cumplimiento de los 114 controles del Anexo de la Norma ISO 27001, según se describe detalladamente en el mencionado informe.

Por lo indicado, la Oficina de Control Interno recomienda establecer un Plan de Acción que permita cerrar las brechas identificadas en el mencionado informe, con indicación clara de la norma que se debe cumplir, los productos esperados, los recursos que se destinan para ello y los plazos para su ejecución. Respecto a los plazos de implementación, se recomienda que los mismos sean establecidos dentro de la vigencia 2019 y 2020, a más tardar, en consideración a que las brechas identificadas son bastante significativas. Es importante señalar que todas las auditorías internas deben registrarse dentro del Plan Anual de Auditorías de la vigencia, como quiera que la Oficina de Control Interno no tuvo conocimiento de la referenciada Auditoría sino con motivo de la elaboración del presente informe.

En este aspecto, cabe reconocer que en el Plan de Acción de la Superintendencia para la vigencia 2019 ya se ha incluido buena parte de las actividades que permitirán superar las brechas identificadas, tal como pudo evidenciarse en la Suite Visión Empresarial.

2) RIESGOS EN MATERIA DE CONTRATACIÓN

El proceso de Gestión Contractual cuenta con tres (3) riesgos identificados en el Mapa de Riesgos Institucional para la vigencia 2019. Los mencionados riesgos son los siguientes:

a) Incumplimiento en el proceso contractual, respecto de la verificación de las garantías exigidas según cada proceso de contratación estatal adelantado por la entidad.
b) No aplicación de las normas y/o procedimientos que rigen la contratación estatal adelantada por la entidad.
c) Recibir dádivas para favorecer a terceros en procesos de contratación.

Para cada uno de los riesgos identificados se definieron acciones para ser ejecutadas durante la vigencia 2019, las cuales se han ido realizando según se evidencia en los reportes de la Suite Visión Empresarial.

No obstante, para los riesgos **uno** y **dos** se definió un entregable concreto que consiste en un *"Seguimiento mensual del proceso de contratación"* (Subrayado fuera de texto), que hace referencia a un *"Acta"*. No se evidencian los reportes de ejecución de esta actividad de los meses de enero a junio de 2019 en la Suite Visión Empresarial. Por lo señalado, es importante que el área de Contratos revise este seguimiento y suba a la SUITE los soportes correspondientes.

De otro lado, una vez verificados los procesos de contratación actualmente publicados en el SECOP por parte de la Superintendencia, se evidencia que todos cuentan con matriz de riesgos específica para cada proceso. Se evidencia que la Entidad realiza los análisis de sector relativo a cada proceso de contratación y que efectúa la evaluación del Riesgo utilizando los documentos definidos por Colombia Compra Eficiente, teniendo en cuenta las indicaciones establecidas en la Circular Externa Única de 2019 de la Agencia Nacional de Contratación Colombia Compra Eficiente. En relación con estos riesgos, consideramos importante verificar los controles aplicados para el riesgo b), como quiera que según

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Omar Urrea Romero
Revisado para firma por	Sandra Milena Neira Sánchez
Los arriba 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 la firma.	

informe de auditoría elaborado con la oficina de Control Interno se identificaron debilidades en el cumplimiento de la norma contractual.

3) RIESGOS EN MATERIA DE SEGURIDAD Y SALUD EN EL TRABAJO

El proceso de Talento Humano cuenta con tres (3) riesgos identificados en el Mapa de Riesgos Institucional para la vigencia 2019. Los mencionados riesgos son los siguientes:

a) No atender de manera oportuna los accidentes, incidentes y/o enfermedades laborales, así como las urgencias y/o emergencias de la Entidad.
b) No garantizar los derechos laborales de los trabajadores de la entidad.
c) Pérdida de recursos públicos por la inasistencia de las actividades programadas en los planes.

Para cada uno de los riesgos identificados se definieron acciones para ser ejecutadas durante la vigencia 2019, las cuales se han ido realizando según se evidencia en los reportes de la Suite Visión Empresarial.

En cuanto al primer riesgo, relacionado con el tema de accidentes, incidentes y enfermedades laborales, se tiene como control ejecutar la siguiente actividad: *"Hacer seguimiento trimestral al Plan Anual del Sistema de Gestión del Sistema de Seguridad y Salud, de acuerdo a las etapas establecidas y al Decreto 1072 y a la Resolución 1111"* (Subrayado fuera de texto). No obstante, a la fecha no se evidencia en la SUITE el informe de seguimiento correspondiente al primer y segundo trimestre de 2019.

De otro lado, en relación con el Sistema de Gestión de Seguridad y Salud en el Trabajo de la Superintendencia, se evidencian los siguientes avances en el primer semestre de 2019:

La entidad realizó la actualización del procedimiento para el reporte e investigación de accidentes e incidentes de trabajo, con la finalidad de especificar como se debe realizar adecuadamente un reporte de Accidente o Incidente Laboral, igualmente se definió el responsable de entregar la información a la A.R.L. Lo señalado pudo evidenciarse en la SUITE.

Se estableció un Programa de Prevención y Protección de la Seguridad y Salud de las personas, aprobado en el Sistema de Gestión de Calidad de la entidad. Las actividades definidas en este programa buscan fortalecer la prevención de la salud de los trabajadores de la Entidad. Se evidencia que el mencionado programa fue elaborado con la asesoría de la ARL Positiva SA.

El Sistema de Gestión de Seguridad y Salud en el Trabajo cuenta con el Reglamento de Higiene y Seguridad Industrial y la Matriz de Peligros o matriz de riesgos específico debidamente diligenciada y publicada en la SUITE de la Entidad. Todos los riesgos identificados cuentan con la valoración correspondiente, están contenidos en la matriz exigida por el Sistema de Seguridad y Salud en el Trabajo y tienen definidas actividades para su mitigación. La información está disponible en la SUITE visión empresarial de la Superintendencia. No se tienen observaciones específicas a este respecto.

RECOMENDACIONES

La Oficina de Control Interno recomienda adelantar las siguientes actividades para efectos de contar con un Mapa de Riesgos actualizado y con acciones cumplidas y reportadas a través de la SUITE. Lo anterior, particularmente en los casos de: 1) Seguridad de la Información, 2) Contratación y, 3) Seguridad y Salud en el trabajo.

a) Se recomienda al área de Sistemas avanzar en la consolidación y ejecución del Plan de Acción para implementar las medidas para el cierre de brechas en el cumplimiento de la Norma ISO 27001 de 2013 y su Anexo correspondiente, de acuerdo con los resultados de los informes finales de los contratos celebrados con las empresas Globaltek Security S.A.S. y MNEMO Colombia SAS, arriba descritos. A este respecto, es recomendable que se realice un seguimiento específico para cada una de las

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Omar Urrea Romero
Revisado para firma por	Sandra Milena Neira Sánchez
Los arriba 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 la firma.	

recomendaciones de los mencionados informes y que se deje evidencia del cumplimiento de cada una de las acciones que se han formulado para lograr el cierre de brechas identificadas por las empresas externas.

b) Se recomienda al área de Contratos verificar los seguimientos y controles a los riesgos identificados en la SUITE para este proceso y actualizar los reportes de avance a junio 30 de 2019.

c) Se recomienda al área de Talento Humano verificar los seguimientos a los riesgos identificados en la SUITE para este proceso y actualizar los reportes de avance a junio 30 de 2019, en particular los reportes de seguimiento trimestral al Plan Anual del Sistema de Seguridad y Salud en el Trabajo.

PLAN DE MEJORAMIENTO

De acuerdo con los resultados obtenidos, no es necesario formular un Plan de Mejoramiento específico en los temas objeto de análisis. Lo anterior, siempre y cuando las tres recomendaciones señaladas en el capítulo anterior sean atendidas por parte de las áreas señaladas.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Omar Urrea Romero
Revisado para firma por	Sandra Milena Neira Sánchez
Los arriba 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 la firma.	