SINDICATO SINDHEP
COMUNICADO PÚBLICO N°07
Fallas de Seguridad Ponen en Riesgo la Información en la Defensoría del Pueblo-Colombia

Desde hace algunos días, los servidores públicos de la Defensoría del Pueblo, han recibido en sus correos electrónicos institucionales, mensajes que amenazan con afectar la seguridad de la información de la entidad, simulando ser citaciones o notificaciones judiciales, pero que al abrirlos, replicarlos o dar clic en los vínculos adjuntos, podrían estarse instalando y transmitiendo virus u otro tipo de contenido potencialmente malicioso.

Pese a la importancia que reviste la protección de la información pública, la Defensoría del Pueblo no cuenta con una Oficina de TIC. Existió hasta el 2014 bajo el amparo de la Ley 24 de 1992, no obstante, la reforma administrativa del Decreto 025 del 2014 la eliminó de la estructura organizacional.

Además de esta falencia, en un mundo gobernado por las tecnologías de la información, tampoco existe claridad funcional frente a los roles y responsabilidad por la administración del Sistema de Gestión de Seguridad de la Información -SGSI-, de la política de seguridad, los estándares ni los procedimientos de TI, pues el profesional especializado designado mediante acto administrativo como responsable de grupo de trabajo en TIC, fue desplazado funcionalmente por la administración de Camargo con la Resolución No. 262 del 14 de febrero de 2022, que designó arbitrariamente roles de coordinación generando duplicidad funcional en cargos que ya habían sido creados con este propósito de acuerdo al Decreto 026 de 2014, afectando también la jerarquía funcional.

La reforma del 2014 dejó como consecuencia unas funciones que ahora desarrollaría un grupo interno de trabajo, que son áreas funcionales, éstas con subordinación de la Secretaría General

y no como una oficina asesora con dependencia directa del Defensor del Pueblo, como lo disponen las buenas prácticas, la lógica de la administración pública y la normatividad vigente en materia de TIC.

Esta falta de claridad y afectación en materia de TIC ha llevado a reiteradas ventanas de mantenimiento, donde los sistemas de información dejan de funcionar y presentan fallas por causas que van desde vencimientos de licencias de software hasta infiltraciones y captura de información por parte de terceros en los correos institucionales de los servidores públicos.

Ante esta situación, la administración ha respondido con comunicaciones internas a los correos institucionales en la que conmina a los servidores a cumplir con las políticas de seguridad de la información, y a sacar copias de seguridad, dejando el mensaje de que son los funcionarios, contratistas y proveedores los únicos responsables, pero no asumen las falencias estructurales que son deber de la administración.

De acuerdo a la normatividad vigente y las buenas prácticas en materia de TIC, se debe designar un Oficial de Seguridad de la Información, que asuma la responsabilidad de la administración de la seguridad, pero la duplicidad funcional y la ambigüedad jerárquica impide esta designación: "*La administración de la seguridad incluye realizar monitoreo de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en la entidad causado por vulneraciones o incidentes de seguridad*". (Tomado de: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf)

Es preciso que el Defensor del Pueblo reconozca que la responsabilidad por la administración de los activos de TIC le corresponde a su administración, y que no es lo mismo "seguridad informática" que "seguridad de la información". La primera es su responsabilidad, la segunda le compete tanto a servidores públicos, como contratistas, proveedores y a también a la administración. La llegada masiva y repetida de correos con contenido malicioso es evidencia de que la seguridad informática está siendo vulnerada y la información está en riesgo.

Igualmente, se están presentando fallas permanentes en otros sistemas de información y plataformas de registro documental misional y de gestión administrativa como **VISIONWEB, ORFEO, SISAT**, lo cual obstaculiza y ralentiza el trabajo misional de los funcionarios, pues no pueden tramitar los casos en la jornada laboral, viéndose obligados a trabajar hasta altas horas

de la noche o fines de semana para avanzar en el trabajo, como resultado hay sobrecarga laboral, estrés y otros problemas de salud ocupacional que no están siendo atendidos por la Defensoría del Pueblo.

La situación, además de lo anterior, es crítica frente a la Atención Defensorial, el corazón de la misión institucional, explicada y estructurada funcional y procedimentalmente en la **Resolución N°396 de 2003**, ya que al expedir actos administrativos de adopción de políticas de "Integración Misional y Administrativo", fusionan peticiones, quejas y asesorías propias de la misión institucional de las Direcciones Nacionales de Atención y Trámite de Quejas (ATQ), y de Recursos y Acciones Judiciales (RAJ), con las peticiones y quejas propias de la ley de Transparencia (PQRS), que anula el valor procedimental y el efecto normativo de la citada Resolución que adoptó el "**Instructivo General de Atención Integral de la Defensoría del Pueblo".**

El artículo 7º. de la Resolución 772 de 2020, *por el cual se reglamenta el ejercicio del derecho de petición y el trámite interno de las peticiones misionales y administrativas presentadas ante la Defensoría del Pueblo y el acceso a la información pública*, permite integrar sin distingo alguno las peticiones de tipo misional y administrativo, señala que;

> *"Las peticiones escritas recibidas en las ventanillas de correspondencia se registran en el Sistema de Gestión Documental ORFEO y se remiten a las dependencias competentes, para su trámite en el Sistema de Información Misional - VISIONWEB módulo – RUP - y direccionamiento a los módulos misionales según el asunto y competencias."*

El registro misional duplicado o triplicado realizado a nivel Nacional en los Sistemas de Información VISIONWEB DPU, RAJ y ATQ., trae como consecuencia un aumento exponencial y significativo en el Registro Único de Peticiones – RUP (Misional) y la Atención Defensorial ORFEO (administrativo); informes y estadísticas presentados por el "Grupo de Transparencia" de la Secretaría General, como insumo al Informe Anual al Congreso de la República presentado por el Defensor del Pueblo, información formalizada y justificada para solicitar recursos presupuestales adicionales o aumentos de plantas de personal en el nivel Central y Regional, como el recientemente aprobado por más de 550 funcionarios.

Paradójicamente, esta situación se presenta en el marco de la ejecución del "Programa de Fortalecimiento de la Capacidad Institucional de la Defensoría del Pueblo", financiado con el préstamo del Banco Interamericano de Desarrollo (BID), por un valor de $18.000.000 dólares -

Contrato de Préstamo N°4550/OC-CO-. Habría que preguntarse: ¿Cómo se están invirtiendo estos recursos?

El Defensor del Pueblo, Carlos Camargo, está omitiendo su deber de proteger información sensible y generar información de calidad, que por la naturaleza de la entidad se relaciona con la defensa, la protección y divulgación de DDHH, y en otros casos con la vulneración o violación a los DDHH e infracciones al DIH de poblaciones reconocidas como Sujetos de Especial Protección Constitucional.

También es contradictorio que, las vulneraciones a la seguridad informática institucional se presenten a pocos meses de la compra un Laboratorio Forense de Evidencia Digital, con la capacidad de realizar extracción, y análisis de evidencia digital, al que sólo unos pocos funcionarios tienen acceso, y que casualmente, quien está a cargo del mismo Laboratorio, fue designada como coordinadora por la misma resolución No.262 de 2022 que también desplazo al Responsable del Grupo de Investigación Defensorial (Profesional Especializado Grado 20), al igual que al responsable del grupo de TIC. Es decir, que por un lado se baja la guardia, pero por el otro, se implementa tecnología de punta para obtener información, ¿Qué sentido tiene esto?.

Nuestra colectividad ya ha denunciado con preocupación, el uso y propósitos que cumple el Laboratorio Digital de Evidencia Forense, en punto de su utilización para vigilar y amedrentar a funcionarios de la entidad, y según lo antes manifestado, la actuación de la administración continúa ofreciendo indicios que reafirman estas preocupaciones. De esta forma, mientras se baja la guardia en la seguridad informática, crece la vigilancia al interior de la Defensoría del Pueblo, al punto de emular las funciones de la Fiscalía General de la Nación, y aumenta considerablemente el presupuesto para la seguridad del Defensor del Pueblo.

Esta serie de hechos nos convoca como servidores y servidoras públicas, asociados en SINDHEP, a hacer un llamado a los órganos de control para que intervengan:

- A la Contraloría General de la República, Procuraduría General y Fiscalía General de la Nación, adoptar las medidas pertinentes con relación a la responsabilidad que le corresponde al Defensor del Pueblo, Carlos Ernesto Camargo Assis, en caso que esté omitiendo su deber de proteger la información pública que maneja la Defensoría del Pueblo, con el agravante que es información sensible referente a violaciones de derechos humanos e infracciones al Derecho Internacional Humanitario de población vulnerable, en su mayoría reconocidos como Sujetos de Especial Protección Constitucional.

- A la Contraloría General de la República para que realice una Auditoría de Cumplimiento con relación a los propósitos definidos en la destinación dada a los 18 millones de dólares del préstamo otorgado por el BID.
- Al Ministerio de TIC y a la Contraloría General de la República para que realice un Diagnóstico pericial de la situación administrativa, funcional, procedimental, jurídica y, tecnológica, en la que se encuentra actualmente el Grupo de TIC, que a pesar de no tener visibilidad en el organigrama de la Entidad es considerado en los Estudios Técnicos de Solicitud del Recurso Presupuestal y de Personal, estratégico en tanto conserva todas las funciones y actividades de una Oficina de Sistemas legalmente constituida.
- Al Ministerio del Trabajo, se adopten medidas con relación a los impactos que dichas dificultades en materia de TIC están provocando en el bienestar de las y los trabajadores ante el mal funcionamiento de las plataformas VISIONWEB Y ORFEO, que implica estrés laboral por la inestabilidad de los sistemas de información, sobrecarga de trabajo, realizar el registro en la plataforma fuera de la jornada de trabajo, etc.
- A la Subdirección de Gestión del Talento Humano de la Defensoría del Pueblo, para que haga extensiva esta comunicación a la Administradora de Riesgos Laborales Positiva y al Comité Paritario de Seguridad y Salud en el Trabajo (COPASST), y sea analizada la situación y se reciba la asesoría técnica para implementar los correctivos en relación con la Seguridad y Salud en el Trabajo.

24 de febrero de 2023

CONSEJO DE GESTIÓN
SINDICATO DE DEFENSORAS Y DEFENSORES DE DERECHOS HUMANOS DE LA DEFENSORÍA DEL PUEBLO