INFORME AUDITORÍA DE SEGUIMIENTO AL PLAN DE MEJORAMIENTO DEL PROCESO DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA

En cumplimiento del Plan de Auditorías de la Oficina de Control Interno –OCI-, y en desarrollo de los objetivos generales y específicos, se realizó la apertura a la auditoría de seguimiento al proceso de **Sistemas de Información e Infraestructura** el martes 26 de julio 2022. En esta sesión se dieron las pautas para iniciar la revisión por parte de la OCI, teniendo en cuenta el Plan de Mejoramiento suscrito el 30 de junio 2021 con la Oficina de Informática y Telecomunicaciones actualmente Dirección de Tecnologías de Información y Comunicaciones, GIT Gestión del software - GIT Infraestructura Tecnológica (actual Subdirección de Infraestructura Tecnológica), producto de la auditoría integral realizada en la vigencia 2021, con entrega de informe mediante memorando con Radicado No. 1500-2021-0000164-IE-001 (caso No. 122349) del 30 de junio de 2021. En este sentido, se obtuvo el siguiente resultado:

El Plan de mejoramiento suscrito contempló tres (3) oportunidades de mejora, donde se plantearon tres (3) estrategias, las cuales presentan un avance del **100%** a la fecha de realización del seguimiento. Por lo tanto, se obtiene una calificación de cumplimiento de **5.0**, en un rango de 1 a 5., para los siguientes hallazgos:

OPORTUNIDAD DE MEJORAMIENTO SEGÚN RESULTADO DE LA AUDITORÍA 2021	ESTRATEGIA	RESPONSABLE	CALIFICACION
1. Realizar revisiones periódicas al software instalado en los equipos de cómputo del IGAC, para evitar la instalación / U50 de aplicativos que no autorizados (WinRAR, Dropbox, iTunes, Ccleaner, etc.), ocupando espacio en los discos duros , generando riesgos de seguridad informática.	Trimestralmente se realiza una revisión al software instalado en los equipos de cómputo por cada proceso del IGAC. (Se revisa una muestra)	Hermes Ramírez	5.0
2. Realizar el análisis de los reportes periódicos que generan los dispositivos de monitoreo de la infraestructura tecnológica del IGAC y documentar la información de las acciones que	Trimestralmente el GIT de Infraestructura genera un informe de las acciones de monitoreo de la infraestructura	Luis Fiorenzano	5.0

OPORTUNIDAD DE MEJORAMIENTO SEGÚN RESULTADO DE LA AUDITORÍA 2021	ESTRATEGIA	RESPONSABLE	CALIFICACION
garanticen la contención, mitigación, erradicación y no repetición, de los eventos y alertas.			
3. Se observa que para la vigencia 2021 la Oficina de Informática y Telecomunicaciones no ha realizado la actualización del PETI	Actualizar y aprobar por el Comité Institucional de Gestión y Desempeño el documento PETI.	Guillermo Gómez	5.0

RESULTADOS SEGUIMIENTO

Puntaje obtenido **15** de **15** puntos posibles**,** equivalente a un avance real del **100%**

COMENTARIOS AL SEGUIMIENTO

SUBDIRECCIÓN DE INFRAESTRUCTURA TECNOLÓGICA

1. Para este hallazgo, se evidenció carpeta “1.RevisionSW” subdividida por vigencias (2021 – 2022), donde la Subdirección de Infraestructura Tecnológica presenta para cada trimestre archivo con el informe de implementación de estrategias de seguridad y monitoreo de control de aplicaciones del trimestre correspondiente. Es decir, los dos últimos de la vigencia 2021 y el primero de 2022, teniendo en cuenta que la fecha máxima de ejecución de la actividad era nueve (9) meses, a partir de la fecha de firma de plan de mejoramiento, así:

    - Informe implementación de estrategias de seguridad y monitoreo de control de aplicaciones del tercer trimestre del 2021 (10 páginas).
    - Informe implementación de estrategias de seguridad y monitoreo de control de aplicaciones del cuarto trimestre del 2021 (14 páginas).
    - Informe implementación de estrategias de seguridad y monitoreo de control de aplicaciones del primer trimestre del 2022 (5 páginas).

2. Para este hallazgo la Subdirección de Infraestructura Tecnológica presenta carpeta “2.RevisionMonitoreo” subdividida por vigencias (2021 – 2022), donde para cada trimestre,. Se evidenciaron archivos con los informes mensuales (clasificados

confidenciales), de búsqueda de información en redes sociales, tales como Facebook, Youtube, Instagram, entre otros, y el de monitoreo del SOC (Centro de Operaciones de Seguridad)[1] el cual analiza los eventos en busca de patrones de comportamiento inusuales distribuyéndolos entre eventos e incidentes y los clasifica dentro de las reglas de correlación previamente configuradas. Estos detectan eventos e incidentes de tipo tales como: descarga de ejecutables sospechosos provenientes de un sitio de mala reputación; actividad de escaneo en la red, en función de descubrimiento de puertos; violación, infracción y vulneración de políticas de seguridad; detección de malware, así:

Archivo	Páginas
210805 Informe Redes Sociales IGAC Julio	22
210805 Informe SOC IGAC Julio	14
210905 Informe Redes Sociales IGAC Agosto	24
210905 Informe SOC IGAC Agosto	16
211006 Informe Redes Sociales IGAC Septiembre	22
211006 Informe SOC IGAC Septiembre	20
211109 Informe Redes Sociales IGAC Octubre	27
211109 Informe SOC IGAC Octubre	20
211213 Informe Redes Sociales IGAC Noviembre	25
211213 Informe SOC IGAC Noviembre	25
220104 Informe Redes Sociales IGAC Diciembre	24
220103 Informe SOC IGAC Diciembre 2021	26
220208 Informe Redes Sociales IGAC Enero 2022	27
220208 Informe SOC IGAC Enero 2022	43
220315 Informe Redes Sociales Febrero IGAC	38
220315 Informe SOC IGAC Febrero 2022	21
220404 Informe SOC IGAC marzo 2022	23
220415 Informe Redes Sociales IGAC marzo 2022	46

3. Se evidencia carpeta “3.PETI” que contiene cuatro archivos, a saber:
   - Plan Estratégico de Tecnologías de Información – PETI 2018 – 2022 versión 3 (130 páginas), actualizado el 1 de diciembre de 2021
   - Anexos A - Plan Maestro Detallado y B - Presupuesto (52 y 1 páginas, respectivamente)
   - Acta No. 13 de 2021 que en el punto “2. Aprobación de:”, el Comité Institucional de Gestión y Desempeño aprueba el PETI 2022 el 30 de diciembre de 2021.

[1] Secutiry Operation Center. Plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas. Su objetivo principal es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas. (https://www.oracle.com/es/database/security/que-es-un-soc.html)

CONCLUSIONES

- Se evidenció el compromiso por parte de la Dirección de Tecnologías de Información y Comunicaciones en el cumplimiento de cada uno de los hallazgos de la Auditoría de Gestión realizada en el 2021 y la implementación de estrategias adecuadas al Plan de Mejoramiento, suscrito el 30 de junio 2021 con la Oficina de Control Interno. Se tiene un avance del 100%, sumatoria correspondiente al cumplimiento de tres (3) estrategias planteadas para subsanar los tres (3) hallazgos producto de la auditoría de 2021.

- Se observó cumplimiento al hallazgo No. 1, conforme a los informes trimestrales presentados acerca de implementación de estrategias de seguridad y monitoreo de control de aplicaciones.

- Se evidenciaron como soportes para subsanar el hallazgo No.2, los reportes periódicos que generan los dispositivos de monitoreo de la infraestructura tecnológica del IGAC, con los informes de utilización de redes sociales y del SOC.

- La Dirección de Tecnologías de Información y Comunicaciones, actualizó, gestionó, y validó el Plan Estratégico de Tecnologías de Información – PETI 2018 – 2022, de acuerdo a la tercera estrategia propuesta en el Plan de Mejoramiento.

RECOMENDACIONES

- Es importante y conveniente seguir trabajando en mejora continua, para que este tipo de hallazgos no se vuelvan a presentar en las próximas auditorías.

- Se requiere mantener la disposición de la Dirección y Subdirecciones, aportando las evidencias de forma completa y en los tiempos acordados con la Oficina de Control Interno para emitir oportunamente los conceptos.

Adriana Paola Serrano

ADRIANA PAOLA SERRANO QUEVEDO
Jefe Oficina de Control Interno (E)

Proyectó: Diana J. Mora S.