

 IGAC <small>INSTITUTO GEOGRÁFICO AGUSTÍN COLOMBI</small>	INFORME DE CONTRATISTA		FO-GCO-PC02-05
			Versión: 1
			Vigente desde: 01/04/2022

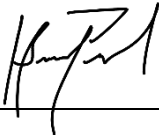
1. DATOS DEL CONTRATO			
Contrato No.	30257 DE 2024		
Nombre del Contratista y/o Representante Legal	HECTOR PERDOMO ANDRADE		
Nombre del supervisor y/o interventor	ROBERTO CARLOS PANTOJA BENITEZ		
Dependencia	SUBDIRECCIÓN DE INFRAESTRUCTURA TECNOLÓGICA.		
Objeto del contrato	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA REALIZAR LA GESTIÓN DE LAS HERRAMIENTAS DE SEGURIDAD DE PROTECCIÓN AVANZADA, SOC/NOC ANÁLISIS DE VULNERABILIDADES Y DETECCIÓN DE AMENAZAS EN PROCURA DE APOYAR EL FORTALECIMIENTO DE LA GESTIÓN INSTITUCIONAL DEL IGAC		
Fecha de inicio	25-01-2024	Fecha de terminación	24-12-2024
Período objeto del informe	Del 31-08-2024 Al 30-09-2024		

2. INFORME PARCIAL DE EJECUCIÓN			
No.	Obligación contractual	Actividad desarrollada	Observaciones / Evidencia
2	Activar, colocar en funcionamiento, gestionar y administrar herramientas tipo Soc con el fin de identificar y bloquear las ciber amenazas en la red.	2.9.1 Se realizó la Integración de 35 fuentes adicionales para el monitoreo por protocolos OMI, SNMP.	2.9.1 Actualización fortiSIEM Evidencias: 2.9.1 Actualización fortiSIEM Evidencias Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdeInformacinyLasComunicaciones/Ej2pSHmEhbVOqCQj8ovBjPIB32EBIsE2yjjlQM2rdN5_RQ?e=e0aQeC
3.	Definir, planear y aplicar técnicas de análisis forense, criptografía, ingeniería inversa, hacking ético y auditoría informática con el fin de fortalecer la seguridad en los servidores, sistemas, sistemas de bases de datos y redes de la entidad.	3.9.1 durante este mes se realizó ejercicio de hacking ético a 1 servicios de pruebas, en los cuales se identificaron falencias, se dieron las recomendaciones necesarias para cada uno de los sitios, con el caso 314769.	3.9.1.1 Análisis de vulnerabilidades Evidencia: 3.9.1.1 Análisis de vulnerabilidades.docx Ruta: https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdeInformacinyLasComunicaciones/EV69DLCodq9Oh75SjS9Vcu4B-2OcC2jRCh5rxocjlelFg?e=jTEmrc
4.	Desarrollar técnicas y planes de prevención de riesgos.	4.9.1 Se realizan análisis de los reportes generados por Windows defender, para ejecutar actividades de remediación de vulnerabilidades detectadas en los diferentes sistemas operativos con los que cuenta el IGAC (Windows 7-11, Windows Server, Linux) Se realiza la ejecución de 6 tareas durante este periodo.	4.9.1.1 Reportes Evidencia: 4.9.1.1 Reportes Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdeInformacinyLasComunicaciones/Eld3JRkFo_FPuD3i2R8Zu6sBdVFnGPo8NwRgRsOYmJcQLQ?e=eNUJhp
6	Realizar diagnósticos y análisis forenses de los malware y	6.9.1 Vulnerabilities have verified exploit notification:Notificacion Device Vulnerabilidadesexploit notification:Notificacion	6.9.1.1 Vulnerabilities have verified exploit notification:Notificacion

 IGAC <small>INSTITUTO GEOGRÁFICO AGUSTÍN COLOMBE</small>	INFORME DE CONTRATISTA		FO-GCO-PC02-05 Versión: 1 Vigente desde: 01/04/2022
	ataques recibidos a fin de evitar su reincidencia.	<p>- Alta</p> <p>Se realizo el análisis del evento reportado, se tomaron acciones de remediación y creación de loC.</p>	<p>Evidencias:</p> <p>6.9.1.1 Vulnerabilities have verified exploit notification Vulnerabilidades - Alta.docx</p> <p>Ruta:</p> <p>https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdelainformacinyLasComunicaciones/Edlyv1EHO2xNoDh5Hbkg93wBofCmRtU-KoqDdasQm2V0OA?e=YawtEy</p>
7.	Redactar reportes de riesgos e incidentes para la subdirección de infraestructura.	<p>7.9.1. Durante este se realizó seguimiento al reporte de Colcert en el cual registraron cuentas comprometidas de correo electrónico y errores de configuración en el dominio igac.gov.co, se creó caso para mitigar los incidentes, 314259, 314752, 314757 asignados a cada ingeniero encargado.</p> <p>Durante este periodo se identificaron alertas sobre amenazas y vulnerabilidades las cuales se crearon ticket 313379, el cual se lanzó la remediación desde la consola de defender.</p> <p>Durante este periodo se identificaron alertas sobre amenazas y vulnerabilidad crítica de ejecución de script las cuales se crearon ticket 315967, el cual se lanzó la remediación desde la consola de defender.</p> <p>Durante este periodo se atendió el caso 318001, donde usuario reporto alerta de phishing, se valido el link, pero este ya se encontraba reportado por Google como sitio con malware ya estaba dado de baja.</p> <p>Durante este periodo se identificaron alertas sobre amenaza y vulnerabilidad crítica sobre el servidor de Gitlab por la cual se creó el ticket 318283, el cual realizo el parchado el administrador SO Linux.</p> <p>Durante este periodo se identificaron alertas sobre amenaza y vulnerabilidad crítica sobre el Microsoft Publisher por la cual se creó el ticket 318752, el cual realizo el parchado el administrador de herramienta WSUS.</p> <p>Se realizo seguimiento al caso 313377 relacionado en vulnerabilidades de servidores el cual ya fueron subsanadas.</p>	<p>7.9.1.1 defender riesgos.</p> <p>Evidencia:</p> <p>7.9.1.1 defender riesgos</p> <p>Ruta:</p> <p>https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdeLaInformacionyLasComunicaciones/Eved81CJwCdOq4_4H8B70UEBGfA0PT2bGiy0H1LMEM50gQ?e=yf41ze</p>

 IGAC <small>INSTITUTO GEOGRÁFICO AGUSTÍN COLOMBE</small>	INFORME DE CONTRATISTA		FO-GCO-PC02-05
			Versión: 1
			Vigente desde: 01/04/2022
8.	Apoyar en las actividades que la subdirección de infraestructura tecnológica asigne según las necesidades que se presenten de conformidad con la naturaleza del objeto contractual y las obligaciones generales y específicas del contrato.	8.8.1 Se realizaron actividades solicitadas por medio de Tickets, correo electrónico, se atendieron 15 solicitudes, las cuales se requerían permiso para los proyectos como SNC, ESRI, etc, en reemplazo del ingeniero Jeisson Gutiérrez. Se realizó la creación de plan de trabajo para actualizar GLPI del IGAC.	8.9.1.1 otros. Evidencia: 8.9.1.1 Otros Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdelainformacion/Comunicaciones/EjA06ChPz3xAk08HE6mtTFkBk0UP5D9T7eBM3xY7lcyOwQ?e=bGzqMo
5 REPORTE MENSUALES PARA ENTREGAR			
5.1 Informe de actividades. 5.2 Carpeta con evidencia por obligación. 5.3 Planilla de aportes a seguridad social.			

Hago constar que durante el periodo reportado se adelantaron las anteriores obligaciones y/o actividades.



Firma del Contratista

NOTA. El informe presentado, evidencia la ejecución contractual de las actividades sobre las cuales se desplegaron acciones en el periodo correspondiente.