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 31-07-2024 Al 30-08-2024		

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.	2.8.1 se Realizó la actualización del equipo FortiSIEM de la versión 6.1.2 a la versión 7.2.1 por recomendación de fabrica y proveedor, donde se realizo el formateo del equipo completo y se generaron configuraciones necesarias para el funcionamiento de esta versión. Se realizo la creación de casos para la integración de las fuentes Linux y Windows a través del protocolo SNMP, con los tickets 311112, 313813. Se realizo integración de 4 agentes avanzados para los servidores de AD, los cuales se encuentran reportando de manera correcta. Se realizo la creación maquina colector, para el fortisiem, IP 172.18.0.103.	2.8.1 Actualización fortiSIEM Evidencias: 2.8.1 Actualización fortiSIEM.docx Ruta: https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EanTj8frJspBsaJ0uOC9ZecBoqxIILQeuLHX5Tm_qigxyA?e=I2qr9P
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.	3.8.1 durante este mes se realizó ejercicio de hacking ético a 2 servicios de pruebas, en los cuales se identificaron falencias, se dieron las recomendaciones necesarias para cada uno de los sitios, con los casos 311769, 308941.	3.8.1.1 Análisis de vulnerabilidades Evidencia: 3.8.1.1 Análisis de vulnerabilidades Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EuZcJXyAb21AlJiDrARrdMUBuL1nBNp_M1wn8dxYyvLkUQ?e=oRr2Uj
4.	Desarrollar técnicas y planes de prevención de riesgos.	4.8.1 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)	4.8.1.1 Reportes Evidencia: 4.8.1.1 Reportes Ruta:

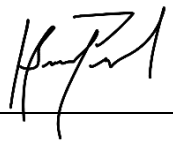
		Se realiza la ejecución de 42 tareas durante este periodo.	https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EpUR1kI_WNlBla7HhCIZNjEB3leyvYzUX8YuE2FgubMXUA?e=4Kc45w
5	Desarrollar y poner en práctica protocolos criptográficos de defensa ante ciberataques.	5.8.1 posterior a análisis de vulnerabilidades se solicitó la creación de un una IP de balanceo aplicando los módulos de seguridad del WAF (F5), para los servicios, ya que se identificaron falencias de seguridad y vulnerabilidades por protocolo SSH. Se dieron todas las recomendaciones necesarias para los servicios, ticket 312849.	5.8.1.1 Ticket Evidencias: 5.8.1.1 Ticket Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/ErigNtYTd8JEgqzErMhvsQwBhjj-lij6z9CNJEimYTxfnQ?e=0kGkBR
6	Realizar diagnósticos y análisis forenses de los malware y ataques recibidos a fin de evitar su reincidencia.	6.8.1 Possible Antimalware Scan Interface (AMSI) tampering was detected by Microsoft Defender for Endpoint on 6004-204960 Se realizo el análisis del evento reportado, se tomaron acciones de remediación y creación de IoC.	6.8.1.1 Possible Antimalware Scan Interface (AMSI Evidencias: 6.8.1.1 Possible Antimalware Scan Interface (AMSI).docx Ruta: https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EfLuJB8vDL1CpgPxTCbroTQBEtuAPMZIP1aiQHQgHc8DKA?e=4cdsPm
7.	Redactar reportes de riesgos e incidentes para la subdirección deinfraestructura.	7.8.1. Se realizo seguimiento al ticket 307883, el cual ya fueron subsanadas las vulnerabilidades identificadas en el mes de julio. Se realizo seguimiento al ticket 307714, el cual ya fueron subsanadas las vulnerabilidades identificadas en el mes de julio. Se realizo seguimiento al ticket 305964, el cual ya fueron subsanadas las vulnerabilidades identificadas en el mes de julio. Se realizo seguimiento al ticket 308630, el cual se encuentra en proceso ya que se requiere validar por parte de los administradores de BD. Se realizo seguimiento al ticket 305776, el cual ya fueron subsanadas las vulnerabilidades identificadas en el mes de julio. Durante este se recibió reporte de Colcert en el cual registraron cuentas comprometidas de correo electrónico y errores de configuración en el dominio igac.gov.co, se creo caso para mitigar los incidentes, 314259, 314752, 314757	7.8.1.1 defender riesgos. Evidencia: 7.8.1.1 defender riesgos Ruta: https://igacoffice365.sharepoint.com/:f:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EozgbQQ_lChPtKUnKpgO8oIBOcMsIxK7ZkfSx7Of-8ODFg?e=vRg8w0

		asignados a cada ingeniero encargado. Durante este periodo se identificaron alertas sobre amenazas y vulnerabilidades las cuales se crearon tickets 313449, 313377, 313379.	
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 realizan actividades solicitadas por medio de Tickets, correo electrónico, se atendieron 5 solicitudes, las cuales se requerían permiso para los proyectos como SNC, ESRI, etc.	8.8.1.1 apoyo subdirección de infraestructura. Evidencia: 8.8.1.1 solicitudes mes de agosto.docx Ruta: https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EbR1bvV7ltpLltLTAI5qznQBInuxkMQA9j7KVqaTSZ7GeQ?e=pgjtHF

5 REPORTES 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.