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	CRISTIAN JOSE PETRO PETRO		
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 01-10-2024 Al 30-10-2024		

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.	2.10.1 Se realizó la creación de dashboard para equipos SNC geográfico. Se crearon alertas para las reglas de los eventos de rendimiento que generen de los servidores SNC geográfico. Se agregaron todos los sitios web, de producción a reglas de STM, para monitoreo y alertas por correo electrónico.	2.10.1.1 FortiSIEM casos de uso: Evidencia: 2.10.1.1 FortiSIEM casos de uso Ruta: https://igacoffice365.sharepoint.com/:f:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/2.10.1.1%20FortiSIEM%20casos%20de%20uso?csf=1&web=1&e=64m1D2
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.	3.10.1 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 318788.	3.10.1.1 Análisis de vulnerabilidades: Evidencia: 3.10.1.1 Análisis de vulnerabilidades.docx Ruta: https://igacoffice365.sharepoint.com/:w:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/3.10.1.1%20An%C3%A1lisis%20de%20vulnerabilidades.docx?d=

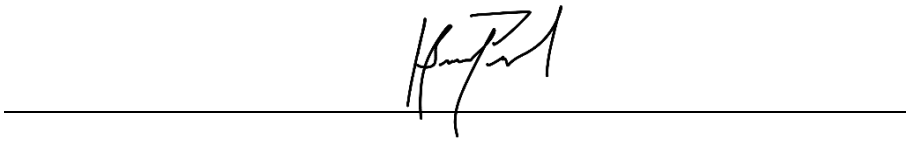
			w30f774e36b11486293bb753868eda28d&csf=1&web=1&e=Gxxodz
4.	Desarrollar técnicas y planes de prevención de riesgos.	4.10.1 Se realizan análisis de los reportes generados por Windows defender, para ejecutar actividades de remediación de vulnerabilidades detectadas en los diferentes sistemas operativos con los que cuenta el IGAC (Windows 7-11, Windows Server, Linux) Se realiza la ejecución de 6 tareas durante este periodo.	4.10.1.1 Reportes Evidencia: 4.10.1.1 Reportes Ruta: https://igacoffice365.sharepoint.com/:f:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/4.10.1.1%20Reportes?csf=1&web=1&e=euIr6s
5	Desarrollar y poner en práctica protocolos criptográficos de defensa ante ciberataques.	5.10.1 Se realizó la encriptación de los registros DMARC sobre el DNS público, con la configuración recomendada por CSIRT.	5.10.1.1 Registro DMARC Evidencia: 5.10.1.1 Registro DMARC.docx Ruta: https://igacoffice365.sharepoint.com/:w:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/5.10.1.1%20Registro%20DMARC.docx?d=wd8d16b46ce0f4b9badc3c8baf83520d9&csf=1&web=1&e=QvQrgX
6	Realizar diagnósticos y análisis forenses de los malware y ataques recibidos a fin de evitar su reincidencia.	6.10.1 Se realizó el análisis del correo electrónico, donde se ingresó al link se descargó el adjunto y se ejecutó en un ambiente controlado, donde se obtuvo información de malware, se dieron las recomendaciones.	6.10.1.1 análisis de correo Evidencias: 6.10.1.1 análisis de correo Ruta: https://igacoffice365.sharepoint.com/:f:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/6.10.1.1%20an%C3%A1lisis%20de%20correo?csf=1&web=1&e=6

			4gc6G
7.	Redactar reportes de riesgos e incidentes para la subdirección deinfraestructura.	7.10.1. Durante este se realizó seguimiento a los incidentes reportados por consola de EDR donde se tomaron acciones sobre eventos críticos.	7.10.1.1 defender riesgos. Evidencia: 7.10.1.1 defender riesgos.docx Ruta: https://igacoffice365.sharepoint.com/:w:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/7.10.1.1%20defender%20riesgos.docx?d=w1c45cde5a2184e4794dfdf19a9e961f3&csf=1&web=1&e=INTkLS
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.	8.10.1 Se realizaron actividades solicitadas por medio de Tickets, correo electrónico, se atendieron 11 solicitudes, las cuales se requerían permiso para los proyectos como SNC, ESRI, etc, en reemplazo del ingeniero Jeisson Gutiérrez. Se realizó apoyo para revisión de la VPN S2S con DANE.	8.10.1.1 otros. Evidencia: 8.10.1.1 Otros Ruta: https://igacoffice365.sharepoint.com/:f:/r/sites/DirecciondeTecnologasdelaInformacinylasComunicaciones/Documentos%20compartidos/Direcci%C3%B3n%20TIC/Contrataci%C3%B3n/P.%20NATURALES/2024/IF-HECTOR%20PERDOMO%20ANDRADE/3.%20Ejecuci%C3%B3n/202410/8.10.1.1%20Otros?csf=1&web=1&e=PDfqAO

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.