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	DANIEL AUGUSTO DUSSAN ROA		
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 31-03-2024 Al 30-04-2024		

2. INFORME PARCIAL DE EJECUCIÓN			
No.	**Obligación contractual**	**Actividad desarrollada**	**Observaciones / Evidencia**
1.	A partir de la orden de inicio del contrato y dentro de los diez (10) primeros días hábiles, deberá elaborar el plan de trabajo y cronograma de actividades indicando el número y tipo de análisis de vulnerabilidades a realizarse durante el mes, así como las actividades para poner en funcionamiento las herramientas de Soc.	1.4 Se elaboro un plan a de trabajo durante este periodo para determinar los pasos a seguir y cumplir con cada uno de estos pasos.	1.4.1 plan de trabajo 1.4.1 plan de trabajo mes de abril.xlsx
2.	Activar, colocar en funcionamiento, gestionar y administrar herramientas tipo Soc con el fin de identificar y bloquear las ciberamenazas en la red.	2.4.1 N/A	2.4.1 Durante este periodo no se realizaron actividades
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.	3.4.1 Se realizo trabajo de análisis a servicio web con herramientas open source bajo marco owas top then	3.4.1 Anexo ticket de con resultados https://mesadeayuda.igac.gov.co/glpi/front/ticket.form.php?id=291268
4.	Desarrollar técnicas y planes de prevención de riesgos.	4.4.1 se solicitó ventana de mantenimiento para realizar actualización de los equipos de seguridad firewall, ya que las versiones firmware tenían varias vulnerabilidades https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-fortios-de-fortinet https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-productos-fortinet-0"""	4.4.1 Se genero actualización de los equipos de seguridad se gestionó con SDC https://mesadeayuda.igac.gov.co/glpi/front/change.form.php?id=70
5.	Desarrollar y poner en práctica protocolos criptográficos de	5.4.1 N/A	5.4.1 Durante este periodo no se realizaron actividades

	defensa ante ciberataques.		
6.	Realizar diagnósticos y análisis forenses de los malware y ataques recibidos a fin de evitar su reincidencia.	6.4.1 se evidenciaron durante este periodo, trafico anómalo hacia servicios de cripto, lo cual se creó caso de seguimiento para identificar evento y equipos que se comprometieron.	6.4.1 generación de reportes de acceso sobre puerto crític https://mesadeayuda.igac.gov.co/glpi/front/ticket.form.php?id=291522&forcetab=Ticket$2
7.	Redactar reportes de riesgos e incidentes para la subdirección de infraestructura.	7.4.1 Se inicio la actualización de los equipos de seguridad con los ingenieros: Nixon Yesid Rubiano Calderon, Jeisson Orlando Gutierrez Samboni Ruben Dario Casallas Hector Perdomo Andrade En el horario de inicio de la ventana 7:00 pm se realizaron las siguientes actividades: 1. Previa Se realizaron los backups del firewall (Fortigate) y manager (Fortimanager). 2. Previa Se realizo actividades de actualización de firmware del fortigate con las versiones 7.0.12, 7.0.16, 7.2.4 3. Previa Se realizo la descarga de los firmware de los FortiManager 7.2.5 4. Previa Se realizo la descarga los firmware de FortiAnalizer version 7.2.5 Las actividades de actualización se realizaron de la siguiente manera: 1. Se realizo actualización del FortiGate sobre las siguientes versiones en escalera 7.0.12, 7.0.16, 7.2.4, 7.2.8 como versión final. 2. Se realizo actualización del FortiManager sobre las siguientes versiones en escalera 7.2.5 3. Se realizo actualización del FortiAnalizer a la versión 7.2.5 Posterior a las actualizaciones de los equipos se realizaron las siguientes validaciones: 1. Ingeniero Nixon Yesid Rubiano Calderón, realizo todas las validaciones de integración con la solución de cisco, todas de manera satisfactoria. 2. Se realizaron pruebas de conectividad de red cableada y wifi, quedando en optimo funcionamiento. 3. Se realizaron validaciones de ingreso a los portales web de la entidad, donde se tuvo acceso sin inconvenientes.	7.4.1.1 todas las actividades se gestionaron mediante SDC https://mesadeayuda.igac.gov.co/glpi/front/change.form.php?id=70

		Se realizaron pruebas de las conexiones VPN, servicios FTP, Navegación a internet. .	
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.	8.4.1 se realizan actividades solicitadas por medio de Tickets, correo electrónico. • Gestión de visualización entre máquinas - ID 291023. • Habilitar conectividad entre LPCJBOSSPRD01 y sitio de internet (www.google.com) - ID 291154 (IGAC) • Actualizacion Firewall - ID 290201 (IGAC) • Comunicación entre máquinas CEM2 - ID 291690 (IGAC) Siguiente Último • acceso a servidores ambiente de capacitacion SNC - ID 291722 (IGAC) • PAGINA METADATOS ICDE - ID 288390 (IGAC) • Test de vulnerabilidades - ID 291268 (IGAC) • SOLICITUD DE MAQUINA WINDOWS SERVER - ID 291038 (IGAC) • SOLICITUD DE MAQUINA WINDOWS SERVER - ID 291038 (IGAC) - ID 292588 (IGAC) • Solicitud actualización clave usuario sncbi en la bd oracle 172.19.1.27 - ID 292383 (IGAC) • Solicitud verificación acceso a pruebasportal.igac.gov.co - ID 293036 (IGAC) • Habilitar acceso en firewall - ID 293680 (IGAC) • Acceso a la BD con usuario de lectura 172.19.1.38 - ID 293299 (IGAC) • Politica SMTP - ID 293506 (IGAC) • Link de metadatos de la pagina de Datos Abiertos - ID 289026 (IGAC • Comunicación entre máquinas ArcGIS Monitor - Oracle - ID 293487 (IGAC)	8.4.1.1 Se realizaron atenciones solicitadas por mesa de servicios, Teams y correo electrónico. https://igacoffice365.sharepoint.com/:w:/s/DirecciondeTecnologasdelaInformacinylasComunicaciones/EQ-vG5EdO3hEj26WiCFJxV4BegDgmgdbjOxKupnxkyt9qQ?e=RSNFlc

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.