0125013822802

N° Radicado **0125013822802**/ MDN-COGFM-JEMCO-SEMPE-CGDJ6-DITIN

Bogotá D.C., 12 de diciembre de 2025

Señor Coronel
Geovanny Andrés Suárez Penagos
Director Administrativo y Financiero CGFM
Comando General Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá D.C.

Asunto: Informe de Supervisión y Seguimiento No 02 del Contrato No. 259-COGFM-DIADF de (2025) Mensual ___ó Final X

Respetuosamente, me dirijo al señor Teniente Coronel , Director Administrativo y Financiero, con el fin de presentar el informe de supervisión y seguimiento del contrato del asunto, de acuerdo con la siguiente información:

1. Datos del supervisor

Nombre del supervisor	Mayor JOSÉ FRANCISCO LOMBANA CARDONA
Dependencia	CGDJ6
Cargo	Jefe Área de Infraestructura
Apoyo a la supervisión	No Aplica

2. Datos del contrato

Número y fecha de suscripción del Contrato	259 COGFM DIADF 2025 del 19 de septiembre de 2025
Contratista	UT 273COGFM H&Y 202
Cedula de Ciudadanía o Nit.	Nit. 901988423-0
Objeto	: PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS

	PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO		
Valor del Contrato	$1.769.215.000		
Plazo de ejecución	12 de diciembre de 2025		
Modificatorio No.			
Adición	Prorroga	Suspensión	Otros
Objeto del modificatorio:			

3. Descripción del desarrollo de las actividades contractuales

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
1	Cumplir con las especificaciones técnicas, estudio previo, el pliego de condiciones y el Contrato, en particular, con los plazos máximos establecidos	x		Se verifica el cumplimiento de las especificaciones técnicas
2	Proveer a su costo, todos los servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el contrato	x		Se verifica que la ejecución del contrato no genere sobre costos para la institución
3	Garantizar que ningún funcionario suministrará ninguna clase de información o detalle a terceros y que mantendrá como documentación clasificada todos los aspectos relacionados con el contrato, así como los asuntos técnicos e instalaciones del Comando General de las Fuerzas Militares, conocidos por el Contratista, durante el desarrollo de este contrato y con posterioridad al mismo	x		El contratista se compromete a cumplir las políticas de seguridad de la información del CGFM
4	Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones derivadas del contrato	x		Se verifica la adquisición de las licencias.
5	Elaborar y suscribir conjuntamente con el supervisor el cronograma de actividades del contrato, dentro de los cinco (05) días calendario siguientes a la comunicación de inicio del plazo de ejecución	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
6	Entregar al Supervisor del Contrato, dentro de los cinco (05) días siguientes al perfeccionamiento del mismo el certificado del curso virtual de cincuenta horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto 1072 de 2015), el cual deberá permanecer vigente durante el plazo de ejecución del contrato	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
	LOTE 2: LICENCIAS PROXY WEB			
	RENOVACIÓN GARANTÍA Y SOPORTE TÉCNICO, LICENCIAS DE LA PLATAFORMA DE SEGURIDAD DE FILTRADO Y ANÁLISIS WEB/PROXY DEL FABRICANTE (FORTINET HERRAMIENTA PERTENECIENTE AL COGFM)			
7	La renovación del licenciamiento es requerida para los siguientes modelos de la solución de seguridad de filtrado web/proxy así: - FPX-2000E: FPX2KET321000015 - FortiAnalyzer VM-GB5 La vigencia de la renovación de las licencias y de la garantía deberá ser de dos (2) años contado a partir del 15 de noviembre de 2025 o fecha que indique la plataforma o documento de fabricante	x		Se verifica el licenciamiento y cumple con las especificaciones técnicas

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
8	Se debe brindar e instalar actualizaciones de la solución de seguridad de filtrado web/proxy descritas en el presente anexo, cada vez que se libere en el mercado una nueva versión de software, Upgrade, Update o parche. Lo anterior previa solicitud y aprobación del supervisor del contrato y una vez haya sido probada en laboratorio, asegurando la continuidad del servicio y funcionamiento de los sistemas	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
9	Se debe realizar entrega al COGFM, de los medios magnéticos o manuales si existen cambios de versión	x		Los manuales digitales de encuentran en la carpeta documentos -> manuales->proxy del equipo del administrador del proxy
10	El servicio de renovación de la solución debe incluir las siguientes actividades de configuración e implementación y puesta en funcionamiento: - Instalación de la última versión establecida por el fabricante - Configuración de la plataforma (direcciones de red, NTP, rutas y demás configuraciones) manualmente. - Aplicar los parches instalados en el equipo - Actualizaciones, Upgrade, Update o parches. - Ajustes a las configuraciones filtros, políticas y excepciones de ser necesario. - Pruebas de identificación de usuarios y de navegación. - Aplicar los controles de navegación a los usuarios del comando general. - Afinamiento de políticas de ancho de banda y priorización de las aplicaciones críticas para el COGFM. - Revisión y afinamiento del control y bloqueo de las solicitudes de DNS contra destinos conocidos y maliciosos. - Afinamiento de la protección contra amenazas de contenido web malicioso como exploits del navegador, scripts e identifique y bloquee botnets y devoluciones de llamada de malware. - Activación de protección antivirus, antispyware y antimalware que se puede adquirir durante la navegación, O en línea. - Nuevas implementaciones.	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
11	Las renovación y activación debe quedar en un esquema 7x24 ante fabricante con las mismas características de seguridad actuales de las plataformas que componen la solución de seguridad de filtrado web/proxy	x		se verifica la activación 7*24 de acuerdo a la certificacion
12	Se debe entregar certificado donde se evidencien las licencias renovadas, con su respectiva clave y fechas de vigencia. (cuando ello hubiere lugar)	x		la certificación del licenciamiento Se adjunto en el informe de supervisión N°1
	SERVICIO DE SOPORTE DE LA SOLUCIÓN DE SEGURIDAD FILTRADO Y ANÁLISIS WEB/PROXY			
13	El Servicio de soporte para la solución de seguridad de filtrado web/proxy debe ser renovado en un esquema y horario 7x24 durante dos (2) años, contado a partir de la fecha de instalación y activación de las renovaciones; siempre y cuando el supervisor lo vea pertinente, cumpliendo las siguientes actividades: - El servicio técnico debe incluir atención de incidentes y consultas de tipo telefónico, correo electrónico (e-mail), acceso remoto, plataforma de mesa de ayuda y atención en sitio (presencial) en la cuidad de Bogotá en caso de que así se requiera, en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado en la solución a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta). - Al finalizar el caso reportado se generará un informe de servicio con las evidencias del antes, durante y después de estas actividades. De igual forma quedará constancia en el informe de servicio si hubo cambio de software y/o en alguna configuración. - El servicio prestado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket o casos reportados para los incidentes presentados en la mesa de ayuda). - Se debe tener una atención ilimitada a casos reportados por el administrador de la solución, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de la solución de filtrado web/proxy, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
14	Durante el periodo de soporte técnico, se requiere un reporte mensual de verificación del correcto funcionamiento de la consola, componente principal de la solución de seguridad de filtrado web/proxy. Las cuales deben incluir como mínimo las siguientes actividades: - Actualizaciones (Upgrade, Update, parches críticos de Seguridad) - Revisión y solución de errores. - Realización y programación de copias de seguridad en la unidad de almacenamiento de la entidad. - Revisión logs - Revisión y Mejoramiento de espacio de disco, Utilización de CPU – RAM. - Desinstalación de funcionalidades inoperativas. - Procedimientos de hardening.	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
15	Una vez realizados los acompañamientos (remotos o en sitio), se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar: - Actividades realizadas. - Actualizaciones aplicadas. - Procedimientos preventivos y/o correctivos aplicados. - Recomendaciones. - Pendientes.	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
16	En caso de presentar fallas en el funcionamiento, continuidad de los procesos y servicios de cada uno de los elementos de software y hardware que componen la solución de seguridad de filtrado web/proxy, se deberán efectuar los soportes todas las veces que se requiera. Estos deben incluir como mínimo: - Instalación y/o reparación de software. - Configuraciones, puesta en producción y funcionamiento. - Cambio de partes y/o repuestos y/o equipos nuevos de ser requeridos de ser necesario. (Servicio que debe ser incluido como garantía extendida con el fabricante.) - Remplazo de equipos por otros de iguales o superiores características en caso de ser necesario. - El tiempo máximo permitido para cambio de partes, repuestos o reparación del equipo es de 20 días calendario una vez sea reportado el incidente, en caso que la falla genere afectación de servicio el contratista deberá suministrar, instalar, configurar y poner en funcionamiento temporalmente un equipo, repuestos o partes de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para COGFM, con el fin de garantizar la continuidad en la prestación de los servicios. - En caso de que el repuesto o reparación del equipo ocasione la reinstalación o reconfiguración de software, sistema operativo o firmware, estas labores deben ser realizadas sin costo adicional para COGFM, garantizando la continuidad de los servicios.	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
	GARANTÍA TÉCNICA Y SERVICIO			el informe por tener información de seguridad reposa en el computador del administrador c://proxy
17	Se deberá brindar el acompañamiento de soporte con un horario 7x24 por el proveedor, por el término de veinticuatro (24 meses) contado a partir de la fecha de activación de la licencia o renovación cada vez que el supervisor del contrato lo requiera durante el término de la garantía	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
18	Se debe brindar soporte técnico por medio telefónico o remoto de forma inmediata en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta)	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
19	El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
20	El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
21	Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado son el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
	ALCANCE GARANTÍA TÉCNICA			
22	El término de la garantía técnica (o garantía legal de conformidad con el art. 7° de la Ley 1480 de 2011), de conformidad con el art. 7, 8, 9 y 11 de la Ley 1480 de 2011. Para los servicios prestados será de veinticuatro (24 meses), contados a partir de la suscripción del acta de recibo a satisfacción de los servicios firmada por parte del representante de la empresa o su representante autorizado y el supervisor del contrato	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
23	Es la obligación, en los términos de la ley 1480 de 2011 de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad, el buen estado y funcionamiento de los productos	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
24	Se deberá garantizar las licencias que están respaldadas por la casa propietaria del software, de la última versión disponible en el mercado, de acuerdo con las especificaciones técnicas exigidas	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
25	Entiéndase como fecha de inicio del contrato instalación, la fecha en que se realice y evidencie la renovación de las licencias, en la respectiva consola de gestión	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
26	El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración y realizar pruebas exitosas de funcionalidad			El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
27	Dentro de los primeros cinco (05) días calendario al inicio del plazo de ejecución, el contratista deberá entregar al supervisor para la aprobación, el cronograma a desarrollar para el cumplimiento del objeto del contrato, donde incluya los recursos necesarios para la ejecución e implementación	x		El certificado de la garantía técnica se adjunto en el informe de supervisión N°1
28	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo son de referencia, en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se realiza la revisión del pliego de condiciones del contrato
	FUNCIONAMIENTO Y CONTINUIDAD			
29	Garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados por los sistemas y equipos descritos en este anexo, a partir de la fecha de activación del producto	x		Se realiza la actualización garantizando el funcionamiento
	SEGURIDAD			
30	ACUERDO DE CONFIDENCIALIDAD: El Contratista y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista, lo cual será verificado por el supervisor del contrato	x		Se adjuntan acuerdos de confidencialidad
31	Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares	x		El contratista se compromete a cumplir con las políticas de seguridad
32	El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando	x		El contratista se compromete a cumplir con las políticas de seguridad

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	General de las Fuerzas Militares. durante el tiempo de ejecución, garantía y soporte que brindará			
	OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO			
33	El contrato debe ejecutarse a todo costo. el contratista se compromete a renovar el Licenciamiento con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad	x		El contrato se ejecuta a todo costo
34	El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará	x		En el informe de supervision N1 se adjunto la certificación de aceptación de politicas de seguridad
35	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia, en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se cumple con las capacidades técnicas para la ejecución del contrato
36	PERSONAL PARA LA EJECUCIÓN DEL CONTRATO - INGENIERO DE SOPORTE: VÍCTOR MANUEL MENDOZA ANAYA, Ingeniero de Sistemas	x		El personal cumple conlas especificaciones
37	En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad: éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario. Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa	x		No fue necesario realizar cambio de personal
38	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto	x		No fue necesario realizar cambio de personal
39	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado	x		Se verifican planillas de pago de seguridad social
40	El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato	x		No fue necesario realizar cambio de personal
41	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el Contratista debió efectuar el respectivo análisis del pliego de condiciones del contrato y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato	x		La ejecución conto con las capacidades necesarias para la ejecución
42	Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se ejecuta el contrato de acuerdo a las especificaciones
43	El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato	x		El contratista cump,e con las normas de seguridad industrial

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
44	El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma	x		El contratista se hizo cardo del manejo del personal a cargo del contrato
	LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS			
	LICENCIAMIENTO			
45	El proveedor debe brindar la suscripción de toda la solución, este deberá ser un modelo por suscripción por un periodo de 24 meses a partir del 02 de noviembre del 2025 para todos los módulos; debe ser entregado al Comando General de las Fuerzas Militares-COGFM de acuerdo con los siguientes productos: - SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) - SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA - SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES - SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES - SUSCRIPCIÓN DE PROTECCIÓN DE DATOS - SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS - SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA	x		La suscripción es emitida por 24 meses por 24 meses de acuerdo al certificación del producto
46	Se requiere que la solución sea cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, contenedores de nube, dispositivos OT inclusive si estos se encuentran distribuidos de forma remota. No se aceptan soluciones que involucren hardware o virtualización. La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía. En caso de que se requieran módulos o funcionalidades adicionales deberían activarse sobre la misma plataforma con el mismo sensor	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy y cumple con las especificaciones tecnicas
47	El proveedor deberá rendir un informe en donde certifique la funcionabilidad de la plataforma, la activación de las suscripciones licencias con sus respectivos soportes; así mismo entregará los certificados de las licencias al Departamento Conjunto de Comunicaciones del COGFM	x		el informe por tener información de seguridad reposa en el computador del administrador c://proxy
	GENERALIDADES DE LA PLATAFORMA			
48	La solución debe contar con las siguientes condiciones generales para su operación y correcto desempeño: - Consola única central 100% nube (cloud) para administración y operación de todos los módulos ofrecidos y futuros. - Sensores/software que serán instalados en estaciones de trabajo, servidores, máquinas virtuales, contenedores o dispositivos OT. - La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola por grupos de direcciones IP.	X		Cumple de acuerdo a la ficha técnica
49	En caso de requerir activación de funcionalidades adicionales no debe requerir nuevos despliegues de producto, ni de sensores o agentes en la infraestructur	x		Cumple de acuerdo a la ficha tecnica
50	Se requiere que se despliegue un sensor/agente único para realizar todas las funcionalidades solicitadas con las siguientes condiciones como mínimo: - Sensor que NO requiera ser reiniciado en su instalación como desinstalación. - El proceso de despliegue del sensor debe ser compatible y tener documentado el uso de plataformas de terceros como (SystemCenter / AWS automatic Deployment / GPO / PowerShell / PDQ) entre otros. - El consumo de recursos del agente debe ser en promedio 1% de CPU, teniendo activas todas las capacidades de detección, prevención y riesgo. No debe tener requerimientos de hardware específicos para su funcionamiento. - El sensor a desplegar en ambientes de OT de ser necesario deber ser el mismo que se utiliza en el ámbito OT. - El sensor a desplegar debe convivir con cualquier otra solución de EPP existente en el ambiente sin causar ninguna incompatibilidad ni lentitud en el dispositivo. - El despliegue del sensor no debe requerir desinstalar las soluciones de EPP existentes en el ambiente y no debe crearse ninguna exclusión para su operación de detección de amenazas	x		Cumple de acuerdo a la ficha tecnica
51	- Los sensores a desplegar NO deben requerir actualizaciones de patrones / firmas / comportamientos de forma completa o parcial.	x		Cumple de acuerdo a la ficha tecnica

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	- La solución debe estar basada en AI/ML (inteligencia Artificial / Machine Learning), No se aceptan combinaciones de modelo de firmas/heristica u otros mecanismos no especificados			
52	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional. - La plataforma debe contar con un "Market Place" para poder realizar las integraciones con terceros mediante API y ver el estado de la integración. También disponer de la posibilidad de realizar la prueba o test de nuevos módulos sin necesidad de nuevos despliegues o autorizaciones de terceros.	x		Cumple de acuerdo a la ficha tecnica
53	La plataforma debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API	x		Cumple de acuerdo a la ficha tecnica
54	- La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días consulta en segundos. - La consola de gestión debe incluir capacidades de analítica mediante motores de AI, incluir para todos los módulos capacidades de SOAR que no implique un licenciamiento independiente y que no se limite su uso en la creación de playbooks de automatización.	x		Cumple de acuerdo a la ficha tecnica
55	La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, auto triage notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros	x		Cumple de acuerdo a la ficha tecnica
56	La plataforma debe permitir la definición de roles personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que deben ingresar a la consola como permitir el acceso mediante MFA e integración con SSO	x		Cumple de acuerdo a la ficha tecnica
57	La plataforma debe estar administrada por una única consola en un ambiente jerárquico basado en padres e hijos. En caso de que la entidad requiera, puede dividirse o ser parte de un sistema de CSIRT/SOC para poder ser gestionada de forma colaborativa delegada. Sin que esto impacte la operación y administración de la plataforma	x		Cumple de acuerdo a la ficha tecnica
58	La plataforma debe contar con un portal de ayuda, webinar y base de conocimiento integrado a la consola para poder ampliar los conocimientos sobre los módulos o webinar para poder aplicar buenas prácticas en el desarrollo de la solución. Como también hacer el escalamiento de casos en caso de requerirse con el fabricante en modalidad 7x24. NO se aceptan plataformas o soluciones que tengan múltiples interfaces o múltiples consolas	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración
59	La consola debe incorporar un mecanismo de autodepuración para eliminar los dispositivos que no se gestionan en un periodo mayor a 45 días calendario o definir una política de retención para poder hacer procesos de autodepuración más acelerados	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración
60	El licenciamiento de la plataforma se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración
61	Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes. Estos tokens deben ser de un único uso y deben ser generados de forma aleatoria para que solo los usuarios con el perfil asociado puedan hacer uso de este token de desinstalación	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración
62	La plataforma debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un arbol de procesos de forma: Gráfica, listado de actividades y líneas de tiempo	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración
63	La plataforma debe poder establecer control o comunicación directa por medio de línea de comandos con los sensores (win/linx/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros, estos accesos directos a los dispositivos se deben validar mediante un acceso de Multi factor conocido como MFA	x		Cumple de acuerdo a la ficha técnica, se verifica en la consola de administración

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	REQUISITOS ESPECÍFICOS DE LOS MÓDULOS			
64	SUSCRIPCIÓN DE ENDPOINT DETECTION & RESPONSE EDR, QUE INCLUYE: - Antivirus de nueva generación y EDR - Antimalware - Firewall Management - Control de dispositivos	x		Se verifica el cumplimiento en la ficha técnica del producto
65	Uso de la inteligencia de amenazas basado en la identificación de como los adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques, como también sus asociaciones, IOCs y vulnerabilidades objetivo, detecciones asociadas en los EDR	x		Se verifica el cumplimiento en la ficha técnica del producto
66	Capacidades de detección y prevención de: - Detección y prevención de virus/malware conocido y desconocido o día cero. - Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades. - Detección y prevención por indicadores de ataque (File-less attacks). - Capacidad de independizar la detección de la prevención por políticas. - Identificación y prevención de actividades sospechosas (procesos, registro, script, comandos, drivers). - Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usado por los ataques de Ransomware basado en comportamiento. - Identificación y prevención de movimientos laterales y Accesos a credenciales. - Identificación y prevención de ataques y explotación de vulnerabilidades día cero.	x		Se verifica el cumplimiento en la ficha técnica del producto
67	Capacidades de detección de TTPs en post ejecución como: - Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP). - Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos	x		Se verifica el cumplimiento en la ficha técnica del producto
68	La plataforma debe tener capacidad de desarrollar actividades forenses como: - Contar con un acceso remoto (vía línea de comandos) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual. - Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos	x		Se verifica el cumplimiento en la ficha técnica del producto
69	Contar con comandos de colección de datos que permitan dar paso a investigaciones. Los comandos requeridos son: - Explorar el sistema de archivos y extraer archivos. - Lista de procesos en ejecución. - Extraer el registro de eventos de Windows. - Consultar registro de Windows. - Enumere las conexiones de red actuales y la configuración de la red. - Extraer la memoria de un proceso (memory dump).	x		Se verifica el cumplimiento en la ficha técnica del producto
70	Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son: - Eliminar un archivo. - Terminar un proceso (Kill process). - Eliminar o modificar la clave o el valor del registro de Windows. - Enviar scripts programados. - Enviar y recibir archivos por demanda	x		Se verifica el cumplimiento en la ficha técnica del producto
71	- La solución deberá contar con la capacidad de aislar una activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación extema a la computadora con excepción a la comunicación con la propia consola de gestión de la solución. - La solución debe hacer un mapeo de alertas basado en el modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).	x		Se verifica el cumplimiento en la ficha técnica del producto
72	- La solución deber tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, estado de la conexión a la consola, tags predefinidos, roles de los dispositivos, esto basado en la meta data de los dispositivos registrados como mínimo. - La organización en grupos de forma automática o manual basado en reglas o filtros de acuerdo a los atributos de los dispositivos.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
73	La plataforma debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como Virus total vía API	x		Se verifica el cumplimiento en la ficha técnica del producto
74	La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales.	x		Se verifica el cumplimiento en la ficha técnica del producto
75	La solución debe contar como mínimo los siguientes elementos de análisis y características: - Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control. - Capacidad de protección aun cuando los equipos no cuenten con conectividad a la nube. - Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente. - Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS. - Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos. - Detección y prevención de explotaciones de tipo Force DEP (Data Execution Prevention), Heap Spray preallocation, Force ASLR (Address space layout randomization), SEH (Structured Exception Handling Ovewrite protection), NULL Page Allocation, Remote library Loading, Untrusted font.	x		Se verifica el cumplimiento en la ficha técnica del producto
76	Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente: - Cadenas ejecutadas dinámicamente vía el cmdlet "invoke-expression". - Comandos vía –EncodedCommand. - Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware. - Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware. - Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware. - Detección y prevención de movimientos laterales. - Detección y prevención de intentos de robo de credenciales. - Detección y prevención de intentos de elevación de privilegios. - Detección y prevención de intentos de uso de "sticky keys". - Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés). - Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe	x		Se verifica el cumplimiento en la ficha técnica del producto
77	El módulo de EDR debe tener una cuarentena de archivos el cual debe integrar un análisis de sandboxing automático sin límite de uso. Esto es cuando un archivo llegue a cuarentena se tenga un reporte de sanboxing con el análisis comportamental	x		Se verifica el cumplimiento en la ficha técnica del producto
78	- Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura, como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas Windows y MAC. - Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento. - Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales. - Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie. - Tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.	x		Se verifica el cumplimiento en la ficha técnica del producto
79	- Se deben contar con dashboards para poder ver la actividad de dispositivos externos como: Audio/video, Imaging, Mass Storge, Mobiles (MTP/PTP), impresoras, Wireless (Bluetooth), Any Class. - Debe permitir configurar de forma personalizada la notificación que le aparece a los usuarios cuando se realizar alguna restricción en el acceso.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	- Capacidad de tomar el control del Firewall nativo de estaciones para sistemas Windows y MAC para la restricción o permisos de puertos, IPs y procesos. - Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de red, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.			
80	- Deberá utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall. - Debe tener la capacidad de poder identificar el tipo de conexión para poder hacer bloqueos de tráfico hacia redes wifi, por ejemplo, y con ello poder restringir de forma granular el acceso dependiendo de la política de la entidad.	x		Se verifica el cumplimiento en la ficha técnica del producto
81	Las reglas de Firewall deben poder definir la localización del dispositivo con ello aplicar políticas de forma contextual, para identificar la ubicación se debe hacer con la definición de: - Tipo de conexión & SSID, IP Gateway, Servidor DHCP, Prueba de resolución DNS, Prueba de certificado Https, Prueba de ping, dirección IP	x		Se verifica el cumplimiento en la ficha técnica del producto
	SUSCRIPCIÓN DE CACERÍA DE AMENAZAS ADMINISTRADA			
82	Debe incluir: - Analítica de telemetría de comportamiento con IA - Inteligencia Artificial - Servicio de cacería de amenazas administrada por parte del fabricante 7x24	x		Se verifica el cumplimiento en la ficha técnica del producto
83	Sistema de detección y respuesta de puntos finales, identidad y nube con monitoreo continuo para poder tener visibilidad de actividad anómala, respuesta y desarrollo de actividad forense para evitar potenciales brechas o compromiso en las operaciones. Se deben integrar un sistema de analitica y correlación para realizar análisis retrospectivos	x		Se verifica el cumplimiento en la ficha técnica del producto
84	- Que permita acceso instantáneo al "quién, qué, cuándo, dónde y cómo" de un ataque. - Que la solución EDR permita detectar incidentes automáticamente sin requerir ningún ajuste o configuración antes de estar en pleno funcionamiento. - Que tenga la posibilidad de realizar búsquedas personalizadas sobre las detecciones que se remontan a 90 días para buscar amenazas de manera proactiva y que los resultados de las consultas se devuelvan en cinco segundos o menos.	x		Se verifica el cumplimiento en la ficha técnica del producto
85	Que brinde protección contra fallas silenciosas (que se producen cuando un ataque se desliza a través de las soluciones de seguridad sin que se active ninguna alarma) y que registre todas las actividades de interés de un equipo tanto en tiempo real como después del hecho	x		Se verifica el cumplimiento en la ficha técnica del producto
86	La plataforma debe permitir realizar investigaciones forenses en tiempo real y retrospectivos basado en (Para estos casos con menús dedicados para): - Host (actividad de procesos, actividad sospechosa, actividad de red, entre otros). - Usuarios (terminar donde ha registrado un usuario, que servicios accede, como y de que tipo fue el registro). - Hash (Búsquedas de ejecuciones de Hash, creaciones, modificaciones). - Direcciones IP. - Grupos de dominios. - Búsquedas por el identificador de sensor. - Búsquedas por contexto de procesos. - Contar con un buscador de consultas para identificar (dispositivos con riesgo, con detecciones criticas, con vulnerabilidades materializables entre otros). - Realizar cacería de amenazas en sensores windows, mac, linux, directorio activo y contenedores. - Realizar una evaluación de Mitre mediante mapas de calor, tácticas en el tiempo. - Líneas de comando y actividad ASEP(Aggregate System Entry Point). - Ejecutables que se ejecutan desde la papelera o carpetas temporales. - Actividad de logon, actividad de powershell, actividad de tareas registradas	x		Se verifica el cumplimiento en la ficha técnica del producto
87	- Debe realizar un diagnóstico de "Zero Trust Assessment (ZTA)" para determinar el estado del equipo en la organización. Es decir que evalué el nivel de seguridad en cuanto parámetros de seguridad del sistema operativo y políticas de seguridad de prevención. - Que permita desarrollar reglas o indicadores que identifican y previenen ataques sin archivos que aprovechan los malos comportamientos y que con el tiempo ajuste y amplíe los indicadores integrados.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	- Debe permitir la creación de Indicadores de Ataque por sus siglas IOA, incluso permita crear reglas de IOA personalizadas en la plataforma, Como bloqueos de procesos, archivos, dominios o IPs dependiendo ejecuciones de comandos archivos o procesos antecesores.			
88	- Para la creación de las reglas personalizadas deberá especificar el "tipo de regla" y seleccionar acciones como: operaciones de creación de procesos, creación de archivos, conexión de red y nombre de dominio. - Para las detecciones de dichas reglas de IOA, tenga la capacidad de buscar las detecciones provocadas por una regla especifica.	x		Se verifica el cumplimiento en la ficha técnica del producto
89	Tener la capacidad de realizar búsquedas proactivas (hunting) para eventos de cambios registrados por la telemetría de la plataforma, en un rango o periodo de tiempo específico ejemplos: - Realizar búsquedas de nuevos servicios o tareas programados a alrededor de un proceso de investigación. - Realizar búsquedas de cambios en llaves de registros, accesos remotos, logins alrededor de un proceso, equipo, IP o dominio específico	x		Se verifica el cumplimiento en la ficha técnica del producto
90	- Visualización de incidentes calificados por la plataforma que correlacione las detecciones y actividades asociadas a los incidentes, asignando el indicador de riesgo del impacto del incidente. - La plataforma debe mostrar en forma gráfica el incidente relacionando los dispositivos impactados, procesos y línea de tiempo en la que ocurren los eventos relacionados tanto bloqueados como observados que tiene relación con el incidente. - La solución debe permitir consultar información de telemetría relacionados con un proceso, tarea o comportamiento para ampliar el proceso de investigación y consulta con un alcance de 7 días historicos.	x		Se verifica el cumplimiento en la ficha técnica del producto
91	- La plataforma debe incluir servicios de fábrica para actividades de threat hunting y MDR para tener búsquedas/investigaciones proactivas sobre detecciones y anomalías en el entorno del cliente. - La solución debe realizar el envío de la telemetría en tiempo real y consultada inclusive aun si los dispositivos están fuera de línea esto por un periodo de al menos 7 días.	x		Se verifica el cumplimiento en la ficha técnica del producto
92	La información de telemetría debe ser colectada 7x24 y esta no debe ser mayor a 40MB por día por dispositivo, la información a tomar debe incluir como mínimo +1100 tipos de eventos entre ellos: - Process - Token info events, Creations, Injections, Grandparent, Parent, Child relationships. - Network - Close, Connect, Listen, Receive/Accept for IP4/IP6. - File - Writes, deleted, rename, open and info. - Registry - ASEP, Updates, Dumps, Impersonation. - User - Logon, Logoff, Failed attempts. - DLL - Injection and reflection attempts. - Detalle de los dispositivos incluido, pero no limitado a: - OS - OU Attributes, Hostname, Device type, OS Version, Manufacturer, Model. - Network - MAC, Local and External IP, Neighbors	x		Se verifica el cumplimiento en la ficha técnica del producto
93	La solución debe permite la configuración de consultas personalizadas utilizando un lenguaje de consulta estándar y documentado, estas consultas pueden ser personalizadas y programadas para poder ser utilizadas como reportes vía correo electrónico	x		Se verifica el cumplimiento en la ficha técnica del producto
94	Deberá ofrecer un servicio administrado de cacería de amenazas capaz de detectar intrusiones, actividades maliciosas y adversarios, realizado directamente por el fabricante por medio de un equipo capacitado y certificado sin necesidad de realizar ningún tipo de VPN o instalación de plataforma de terceros para obtener la información. Este servicio se debe prestar en modalidad 7x24x365	x		Se verifica el cumplimiento en la ficha técnica del producto
95	Como parte del servicio deberá buscar de manera proactiva campañas de malware sigilosas y en caso de existir alguna se notificar según corresponda. El proceso de notificación debe ser vía correo electrónico por medio de la misma consola de gestión y administración de los anteriores módulos presentar: - Reportes de cacería. - Librerías para cacería de amenazas. - Investigaciones documentadas. - Espacio para poder someter muestras para análisis.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
96	El servicio deberá ir más allá de la detección pasiva y automatizada, deberá investigar e incluso responder a indicadores que apunten a ataques. Alertar con recomendaciones de remediación, con un análisis detallado que permita determinar ¿qué sucedió? y ¿cómo? responder al incidente	x		Se verifica el cumplimiento en la ficha técnica del producto
97	Deberá contar con investigaciones retroactivas revisando datos históricos en busca de evidencia de una intrusión. Recopilar artefactos de investigación como direcciones IP, dominios, hashes y otros. Estos artefactos deberán ser cargados a una base de inteligencia propietaria del fabricante y generar alertas en la interfaz de usuario de la plataforma de seguridad ofertada	x		Se verifica el cumplimiento en la ficha técnica del producto
98	El proceso de investigación debe contar con un playbook de investigación y análisis para poder clasificar las detecciones como mínimo: Falso positivo, verdadero positivo, indeterminado, sospechoso	x		Se verifica el cumplimiento en la ficha técnica del producto
99	Se debe tener en la consola de gestión de EDR un dashboard que muestre el número de investigaciones realizadas por el equipo de cacería de amenazas	x		Se verifica el cumplimiento en la ficha técnica del producto
100	Contar en el portal de gestión con una librería de cacería de amenazas, como: tips para hacer consultas, TTPs para ataques cloud, Exfiltración de datos, cacería de DLLs, credenciales no seguras, explotación Web, herramientas de acceso remoto, movimientos laterales en windows	x		Se verifica el cumplimiento en la ficha técnica del producto
	SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES	x		Se verifica el cumplimiento en la ficha técnica del producto
101	Debe incluir: - Diagnóstico continuo de riesgos del AD e Intra ID - Detección y prevención de ataques y anomalías de identidad con el uso de inteligencia Artificial	x		Se verifica el cumplimiento en la ficha técnica del producto
102	El sistema debe inspeccionar profundamente los protocolos de autenticación (NTLM, Kerberos, LDAP, etc.) para ayudar a controlar el uso inseguro de protocolos y reducir el riesgo de amenazas de seguridad, incluido el reenvío de credenciales y el análisis de hash de contraseñas con bases de datos de passowords expuestos, así como la detección de ataques como Kerberoasting, Pass-the-Hash y Golden Ticket	x		Se verifica el cumplimiento en la ficha técnica del producto
103	- El sistema debe unificar la visibilidad de las cuentas y las identidades en la nube (EntraID), remota (VPN) y local (Directorio activo local). - El sistema debe proporcionar una calificación del nivel de riesgo de detecciones, anomalías y auditoria del AD indicando niveles (alta, media, baja). - El sistema debe perfilar el comportamiento de cada usuario y dispositivo en la red, incluidos los usuarios privilegiados y las cuentas de servicio y desarrollar una puntuación de riesgo para cada uno de ellos. - El sistema debe descubrir todos los usuarios conectados al directorio activo, detectar y responder a las amenazas relacionadas con la identidad en tiempo real. - El sistema debe ser capaz de descubrir continuamente todas las categorías de usuarios, incluidos los privilegiados, las cuentas de servicio, los usuarios regulares y las cuentas obsoletas. - El sistema debe rastrear y hacer cumplir la política basada en la identidad del usuario para servidores y aplicaciones confidenciales. Debería descubrir, monitorear y administrar automáticamente las cuentas privilegiadas en la red.	x		Se verifica el cumplimiento en la ficha técnica del producto
104	- La plataforma debe permitir la definición de segmentos como VPNs, Contratistas, redes de servidores, DMZ para que con este contexto se pueda aumentar la visibilidad del tráfico de red que se debe monitorear para hacer la detección de amenazas y determinar su acción para protección, contención o solicitud de verificación de identidad. - La plataforma debe mapear el proceso de "Kill Chain Attack & Defense" de Active Directory para proteger el entorno del AD. - El sistema debe reducir la superficie de ataque mediante la identificación de administradores sigilosos, cuentas de servicio mal utilizadas y comportamiento anómalo de los usuarios. - La plataforma debe incluir informes completos sobre riesgo y cumplimiento con ayudas gráficas. - La plataforma debe utilizar ciencia de datos "Data Science" para la investigación de seguridad interna y para cuantificar el riesgo. Como también debe utilizar información basada en hechos (es decir, niveles de privilegio, alertas de seguridad o inteligencia de amenazas para generar una puntuación de riesgo.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	- La plataforma sebe usar el mismo sensor de EDR para las capacidades de detección y análisis sobre la identidad del directorio activo (En los controladores de dominio).			
105	- El sistema debe informar sobre el estado de las contraseñas para todas las cuentas de usuario, identificará a los administradores ocultos, las cuentas obsoletas y otros problemas que tradicionalmente son difíciles de encontrar. - La plataforma debe permitir realizar un desglose o "drill down" bajo demanda desde una búsqueda personalizada que coincida con una o más características de la sesión. - La plataforma debe correlacionar y analizar automáticamente los eventos de seguridad, dentro del contexto de la sesión de un usuario. - La plataforma debe almacenar información de telemetría de usuario para ser consultada sobre detalles tanto para auditoría como para cacería de amenazas usando un lenguaje para consulta de metadata y telemetría. - La plataforma debe proporcionar capacidades de análisis privilegiado (calcular puntajes de riesgo para cuentas y usuarios privilegiados a través de análisis de comportamiento y correlación de actividad privilegiada con información de vulnerabilidad). - La plataforma debe tener la capacidad de utilizar el aprendizaje automático (Machine Learning) no supervisado para crear y mantener modelos de datos de usuarios, grupos de pares de la organización y comportamiento de los activos utilizando funciones en datos de eventos históricos recopilados durante un período definido por el usuario.	x		Se verifica el cumplimiento en la ficha técnica del producto
106	El módulo de detección prevención de ataques de identidad debe: - Detectar contraseñas codificadas utilizadas por aplicaciones que estén en las GPO. - Detectar la creación y eliminación de cuentas de usuario en un período de tiempo. - Admitir esquemas del AD de varios bosques/dominios. - Permitir agregar empleados ejecutivos, de alto privilegio o en riesgo en listas de seguimiento, como también la posibilidad de agregar password conocidos. - Tener la capacidad de crear flujos de trabajo para automatizar respuestas. - Detectar un cambio de credencial anómalo para un usuario. - Detectar una cantidad anómala de activos a los que se accede dentro de una sesión. - Detectar actividades de inicio de sesión de cuentas revocadas. - Detectar el inicio de sesión del usuario desde múltiples ubicaciones geográficas. - Detectar inicios de sesión exitosos desde cuentas no correlacionadas. - Detectar el inicio de sesión desde una ubicación geográfica rara. - Detectar la actividad de administración de DC (creación/eliminación de cuentas) usando VPN. - Detectar la conexión VPN por parte de un no usuario (cuenta de servicio). - Detectar la conexión VPN por cuenta deshabilitada. - Realizar un seguimiento de las actividades de los usuarios en sesiones desde el inicio hasta el cierre de sesión. - Identificar a los usuarios que realizan cambios de credenciales. - Identificar automáticamente cuentas de servicio mediante aprendizaje automático ML. - Detectar la conexión VPN por cuenta de servicio. - Detectar cuentas humanas que se comportan como cuentas de servicio. - Detectar anomalías de acceso por cuentas de servicio. - Detectar el inicio de sesión interactivo por parte de cuentas que no son de usuario (no correlacionadas). - Detectar el inicio de sesión de un usuario no ejecutivo en un activo ejecutivo	x		Se verifica el cumplimiento en la ficha técnica del producto
	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES			
107	Debe incluir: - Descubrimiento de activos en la red con y sin sensor - Inventario de aplicaciones instaladas y usadas - Listado de accesos exitosos y fallidos a los dispositivos - Gestión de vulnerabilidades	x		Se verifica el cumplimiento en la ficha técnica del producto
108	Módulo que deberá proporcionar la visibilidad el todo el entorno de tecnología de la organización, desde la consola central supervisar todo desde un panel de control	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	para explorar aplicaciones, accesos y activos utilizando datos históricos y en tiempo real que tengan o no tengan el sensor instalado			
109	La herramienta deberá ofrecer inventario de aplicaciones instaladas y usadas, listados de extensiones usadas en los navegadores, las versiones que se están ejecutando para identificar aplicaciones sospechosas o no autorizadas. Adicionalmente deben brindar una clasificación y categorización de fábrica	x		Se verifica el cumplimiento en la ficha técnica del producto
110	Se deberán definir grupos de aplicaciones para poder clasificar las aplicaciones como también se podrán crear IOCs para autorizar o bloquear aplicaciones basadas en hash mediante workflows de manera automática	x		Se verifica el cumplimiento en la ficha técnica del producto
111	La herramienta deberá tener la capacidad de identificar todos los dispositivos en la red, incluso si están protegidos o no por la plataforma. Se deben tener 3 clasificaciones (Dispositivo gestionados, dispositivos no gestionados y candidatos a instalar el sensor, dispositivos no soportados entre ellos (impresoras, Routers, dispositivos OT))	x		Se verifica el cumplimiento en la ficha técnica del producto
112	- Sobre los dispositivos administrados se debe obtener información de estado de salud como uso de CPU, Memoria, espacio libre de disco, entre otros. - La herramienta deberá tener la capacidad de monitorear los logins de todos los usuarios activos en la red, con privilegios de administrador, locales o de dominio, historial de inicio de sesión e información de actualización de contraseña. - Cómo parte de la plataforma unificada, la plataforma de higiene de TI deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint.	x		Se verifica el cumplimiento en la ficha técnica del producto
113	- La herramienta deberá proporcionar información contextual para todos los sistemas, utilizando cuadros de mando, gráficos y funciones de búsqueda para profundizar en los datos de apoyo. Los resultados deberán correlacionarse con los dispositivos que están en línea, fuera de línea o no conectados a la red corporativa. - La herramienta de higiene de TI, deberá utilizar la información de la solución de detección y respuesta de endpoints (EDR) para alimentar los datos de búsqueda. - La herramienta deberá tener la capacidad de minimizar el abuso de cuentas privilegiadas monitoreando el uso y creación de credenciales de administrador.	x		Se verifica el cumplimiento en la ficha técnica del producto
114	- Las búsquedas de inventario deberán realizarse en la nube para no tener ningún impacto en el rendimiento de los equipos o en la red. - Solución de administración de vulnerabilidades automática sin escaneos y siempre activa con datos en tiempo real. Donde se pueda realizar análisis de impacto basado en la determinación de si se dispone de exploits o inclusive si se tienen exploits activos en la organización. - La herramienta deberá ofrecer la gestión unificada de amenazas y vulnerabilidades, como parte de una plataforma integral para prevenir vulnerabilidades y la actividad posterior a la explotación de las mismas. - La herramienta deberá permitir investigar vulnerabilidades y exposiciones comunes (CVE) para examinar los objetivos y perfiles de los actores de amenazas. - La herramienta no deberá realizar escaneos para su funcionamiento, lo cual permita la administración de vulnerabilidades automatizada y siempre activa con datos en tiempo real.	x		Se verifica el cumplimiento en la ficha técnica del producto
115	- Cómo parte de la plataforma unificada, la plataforma de gestión de vulnerabilidades deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint EDR. - La herramienta deberá permitir supervisar continuamente el estado de vulnerabilidad de todos los equipos dondequiera que residan: en las instalaciones, fuera de las instalaciones o en la nube. - No debe requerir dispositivos de hardware ni infraestructura adicionales para su funcionamiento. - La herramienta deberá monitorear todos los equipos a través de un sensor ya sea dentro o fuera de la red, en la nube, en equipos físicos y virtuales. - Debe permitir que los datos estén disponibles a través de un dashboard intuitivo y búsqueda en tiempo real. - Deberá proporcionar el contexto de las amenazas para ver tanto la presencia de una vulnerabilidad como la evidencia de intentos de explotación. - Deberá permitir operar instantáneamente tan pronto como sea instalado, monitoreando e identificando las vulnerabilidades sin necesidad de reiniciar o realizar una configuración compleja.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	- Desarrollar por medio del SOC el programa de gestión de vulnerabilidades a lo largo de todo el ciclo de vida, desde el aspecto fundamental del descubrimiento de activos, pasando por la evaluación y priorización de vulnerabilidades y exposiciones, hasta la corrección eficaz.			
	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS			
116	Debe incluir: - Clasificación de información en tiempo real - Detección y prevención de salida de información sensible - Analítica y correlación de eventos con el uso de Inteligencia Artificial	x		Se verifica el cumplimiento en la ficha técnica del producto
117	Se debe proveer funciones de protección de datos para evitar su fuga utilizando el mismo sensor de EDR, con la misma consola de gestión y sin requerir hacer un nuevo despliegue para activar esta funcionalidad	x		Se verifica el cumplimiento en la ficha técnica del producto
118	- El módulo de protección de datos debe identificar información sensible por medio de patrones de contenido, expresiones regulares o etiquetas de Microsoft y Google. - El módulo debe poder identificar y mostrar los flujos de información por volumen de datos o por número de eventos que coinciden con políticas de protección de datos. Esto de forma gráfica para los vectores de salida tanto web como Dispositivos de almacenamiento USB y uso del copiar en el portapapeles. - Los eventos de salida de información deben indicar el archivo que se detecta en la salida, vector de salida, política, usuario donde se debe llevar al perfil de usuario mediante la protección de identidad, el dispositivo donde se debe llevar a la descripción y detalles del dispositivo.	x		Se verifica el cumplimiento en la ficha técnica del producto
119	- Las políticas se deben asignar a los dispositivos, se debe hacer la asignación varios tipos de clasificaciones, debe tener la posibilidad de hacer identificación por porcentaje de similaridad, bloquear el uso de browsers en caso de tener coincidencia con datos sensibles salientes, personalizar las notificaciones de alertamiento a los usuarios. - Las políticas podrán ser configuradas en modo simulación para realizar entrenamiento de reglas antes de activar la prevención.	x		Se verifica el cumplimiento en la ficha técnica del producto
120	- Se podrán crear patrones de contenido por medio de expresiones regulares, como también indicar la cantidad de veces que puede repetirse una coincidencia. - Se podrá crear grupos de aplicaciones web para poder ser granular en las políticas de protección de datos. - La solución debe tener la capacidad para inspeccionar nuevos formatos de archivos cifrados y detectar intentos de exfiltrar archivos cifrados.	x		Se verifica el cumplimiento en la ficha técnica del producto
121	- Las reglas de protección de información deben tener la opción de creación de detecciones indicando el tipo de criticidad y este debe ser procesado y analizado por Inteligencia artificial para poder generar detecciones de anomalías por volumetría y estado de criticidad. - Las reglas de protección de datos deben tener la opción de almacenar la evidencia de los archivos que coinciden con los patrones de detección de salida de datos, definiendo la cantidad de espacio para evidencias en cada uno de los dispositivos y el porcentaje mínimo de ocupación del disco duro.	x		Se verifica el cumplimiento en la ficha técnica del producto
122	La solución de protección de datos debe tener un panel de control para poder ver los flujos de datos, esto es: origen de la información, medio de salida y canal de salida, indicando por colores las acciones tomadas en volumen de eventos o tamaño de datos	x		Se verifica el cumplimiento en la ficha técnica del producto
123	Por medio de políticas se podrá definir que dispositivos se activa la protección de datos, con esto logrando ser selectivos en dispositivos que no lo requieran	x		Se verifica el cumplimiento en la ficha técnica del producto
	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS			
124	Debe incluir: - Indicadores de compromisos en tiempo real IOCs, - Análisis de Sandboxing automático - Perfiles de grupos o actores de ataques y campañas de ciberseguridad	x		Se verifica el cumplimiento en la ficha técnica del producto
125	Protección de dispositivos, protección de identidad y protección de nube al siguiente nivel que combine sandboxing de malware, la búsqueda de malware y la inteligencia de amenazas en una solución integral. Además, que tenga la capacidad de producir un indicador de Compromiso (por sus siglas IOC) tanto para la amenaza que encontró como para todas sus variantes conocidas	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
126	Inteligencia de amenazas tipo TIP (Threat inteligence Platform) que permita la consulta e inyección de IOCs (indicadores de compromiso) vía API manual o automáticamente. Con actualización en tiempo real	x		Se verifica el cumplimiento en la ficha técnica del producto
127	Debe tener Sandbox en nube, capacidad de enviar muestras para análisis por demanda o automáticamente desde los endpoints para complementar el análisis de muestras desconocidas, al menos 100 muestras mensuales por demanda	x		Se verifica el cumplimiento en la ficha técnica del producto
128	Tener disponible una base de datos de archivos de malware al menos los últimos 5 años para poder hacer consulta y descarga de muestras de malware para estudio e ingeniería inversa por parte del equipo de la organización	x		Se verifica el cumplimiento en la ficha técnica del producto
129	La plataforma debe entregar reportes de inteligencia al menos semanales programados sobre amenazas, campañas y ataques más reconocidos para preparación y conocimiento centralizado en la consola de administración	x		Se verifica el cumplimiento en la ficha técnica del producto
130	Se debe contar con un panel que permita consultar inteligencia de Vulnerabilidades para brindar información sobre nuevas vulnerabilidades con una descripción de su impacto en la plataforma y vinculación a campañas de adversarios en ciberseguridad	x		Se verifica el cumplimiento en la ficha técnica del producto
131	Se deben contar con una sección de servicios para poder tener: resúmenes, violaciones, eventos, fuentes de datos, temas y consultas, integraciones API e interfaces, despliegues, dependencias, librerías, Modelos o Frameworks, datos recolectados	x		Se verifica el cumplimiento en la ficha técnica del producto
132	El módulo de inteligencia debe contar con el listado de actores o grupos para ser analizados de forma continua en la cual se pueda definir IOCs, vulnerabilidades, TTPs de mitre de forma gráfica	x		Se verifica el cumplimiento en la ficha técnica del producto
	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA			
133	El módulo debe incluir como mínimo las siguientes funcionalidades: - Analítica y correlación automática de EDR, ITDR, Data Protection, inteligencia de manera integrada XDR - Sistema de SOAR nativo integrado - Analítica de ciberseguridad BOT de Inteligencia Artificial Capacidad por día de 75GB de ingesta adicional a la que ya se cuenta por identidad y el EDR y tiempo de retención de 3 meses (90 días).	x		Se verifica el cumplimiento en la ficha técnica del producto
134	En la misma plataforma de administración de EDR/protección identidad/ gestión de riesgo, XDR se debe tener la capacidad de ingestión de cualquier tipo de dato/logs sin limitación en el uso de conectores OnPremise o conectores cloud para desarrollar las capacidades de SIEM de nueva generación desarrollando a profundidad las siguientes características en una sola plataforma y en una única consola: - Monitoreo y gestión de Incidentes basado en los diferentes vectores usando AI/ML sin configuración de reglas. - Configuración de reglas de correlación personalizadas clasificando los resultados en detecciones y tipificando de acuerdo al modelo de MITRE Attack (Enterprise o Mobile). - Gestión de eventos para hacer consultas avanzadas, dashbboards mediante operaciones condiciones para poder fortalecer los procesos de cacería de amenazas. - Ingesta de datos por medio de conectores que puedan personalizarse o tenerse configurados para poder parametrizar cualquier fuente de información. - Ingesta de datos con capacidad de respuesta orquestada para los vectores de: EDR / Cloud / Identidad / correo / Navegación Web /Red y/o Firewall con el objetivo de mitigar el impacto de incidentes de seguridad. - Se requiere que se puedan crear flujos de trabajo o "playbooks" de respuesta en un SOAR nativo para poder automatizar acciones. - Integrar una plataforma de inteligencia de amenazas "TIP" (Threat Intelligence Platform) Nativa para enriquecer y tener el contexto de amenazas cibernéticas en las investigaciones, detecciones y correlaciones	x		Se verifica el cumplimiento en la ficha técnica del producto
135	La plataforma de SIEM debe tener la capacidad de activar capacidades nativas de detección y respuesta que no requieran configuración para su integración, pero se requiere que se tengan una o más de las siguientes funcionalidades nativas: EDR / ITDR - Identitity Detection & Response del mismo fabricante que ofrece el SIEM	x		Se verifica el cumplimiento en la ficha técnica del producto
136	La plataforma de SIEM debe tener la capacidad de poder integrar de manera nativa las siguientes capacidades, de acuerdo a la solicitud del presente proyecto: - Inteligencia de amenazas reconocida como lider en el mercado (TIP - Threat Intelligence Platform).	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	- Administración de logs sin usar bases de datos estándares ni bases de datos indexadas, para retención de datos de 3 meses. - Investigación en profundidad basado en telemetría, comportamientos o funciones lógicas como funciones de inteligencia Artificial. - Módulo de reportería personalizada con detalles avanzados para tener filtros gráficos (Mapas de calor, ubicación geográfica, pipes, tendencias, barras, tablas,) que se actualicen en tiempo real en segundos y puedan exportarse en documentos pdf. - Incorporar parámetros para realizar una gestión de incidentes (Delegación de casos, seguimientos, escalamientos, documentación específica de cada situación, triage) - Correlación avanzada y personalizada. - Capacidad de desarrollar casos de uso de cumplimiento mediante personalización de correlación e ingesta de datos personalizados. - Entregar capacidades para realizar cacería de amenazas para extrapolar procesos, tareas, dependencias a partir de artefactos o actividades de comportamiento sobre todo el ambiente. - Basado en lago de Datos flexible y de crecimiento adaptable. - Capacidades de UBEA - User Behavior & Entity Analytics por medio de la protección de identidad solicitado anteriormente. - Conectores y capacidades XDR - Extended Detection and response. - Capacidades de SOAR para orquestación y automatización			
137	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional. - La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.	x		Se verifica el cumplimiento en la ficha técnica del producto
138	- La plataforma de SIEM debe tener la capacidad de crear gráficos de tendencia o de observación de datos que pueda visualizarse en: Tablas, pipes, columnas, mapas de calor, mapas de ubicación geográfica, "sandkey", para poder tener el análisis gráfico los cuales se deben actualizar en tiempo real. También en los gráficos se debe tener opción de hacer consultas y filtros para poder hacer profundización en los eventos. - Los gráficos deben exportarse en formato PDF, pueden exportarse para poder convertirse en un formulario o clonarse o eliminarse	x		Se verifica el cumplimiento en la ficha técnica del producto
139	La plataforma debe permitir la creación de tableros de control que permita: - Realizar seguimiento a tendencias, búsquedas de IOCs. - Seguimiento a las operaciones de seguridad para determinar: Tiempos promedio de detección, tiempos promedio de diagnóstico, tiempos promedio de cierre de incidentes. - Tableros de control de mapas de calor con las TTPs de Mitre para determinar frecuencias, impactos sobre la organización	x		Se verifica el cumplimiento en la ficha técnica del producto
140	La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, "autotriage", notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros	x		Se verifica el cumplimiento en la ficha técnica del producto
141	El módulo de SOAR debe ser parte de la plataforma en la misma consola de SIEM integrada de manera nativa, debe contar con un tablero de gestión para ver las ejecuciones de playbooks de los últimos 30 días que muestre: - Cantidad de ejecuciones de playbooks provenientes de alertas, detecciones o incidentes. - Cantidad de ejecuciones que provengan de aprobaciones de usuarios. - Tendencia de ejecuciones de playbooks completas y fallidas. - Top de ejecuciones por tipo de disparo o iniciación de los playbooks. - Listado de la ejecuciones más recientes y listado de ejecuciones que corren por demanda	x		Se verifica el cumplimiento en la ficha técnica del producto
142	El módulo de SOAR debe contar con una biblioteca de playbooks para poder incorporar sin necesidad de construirlos de cero estos, como también debe tener la opción de importar playbook de objetos .yaml provenientes de comunidades y colaboración del ecosistema	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
143	El módulo de SOAR debe permitir la creación de playbooks como mínimo: - A partir de un evento, alerta, detección, incidente, estado de un dispositivo, detección de una instalación de aplicación, cambios de políticas o auditoria de sistema, estado de seguridad de los dispositivos o de la nube, un evento de identidad como mínimo. - A partir de una tarea programada la cual puede ejecutarse de forma recurrente definiendo una fecha, hora, día, mes. - Por demanda, donde un administrador puede iniciar para poder automatizar una tarea. En este caso se puede crear un esquema de variables para poder personalizar las consultas al sistema	x		Se verifica el cumplimiento en la ficha técnica del producto
144	El módulo de SOAR debe contar con información de la ejecución de cada playbook para entender que actividades desarrolló, comprender los procesos de decisión y poder determinar errores para mejorar en el diseño y respuesta de los mismos. Como también deben contar con un módulo de auditoria para determinar quién o cuando se cambió, modificó, Guardando las versiones de cambio y permitiendo volver a versiones anteriores de playbooks	x		Se verifica el cumplimiento en la ficha técnica del producto
145	La plataforma debe contar con capacidades de establecer conversaciones en lenguaje natural mediante motor de Inteligencia artificial para: - Hacer consultas para buscar información en la plataforma (ej: listados de dispositivos con características especificas, búsquedas de aplicaciones de riesgo, vulnerabilidades, consultas de IOCs, que permiten reducir el tiempo de investigación de los analistas). - Consultar sobre ejecuciones de scripts y explicación en lenguaje natural sobre significados de códigos. - Consultas para poder solicitar las consultas a realizar para acelerar la cacería de amenazas. - Consultas para solicitar apoyo en la creación de flujos de automatización. Esta funcionalidad debe estar disponible para poder ser agregada como apoyo a los consultores de SOC, CSIRT o encargados de analizar o investigar incidentes de seguridad.	x		Se verifica el cumplimiento en la ficha técnica del producto
146	El módulo de SOAR debe tener la capacidad de tomar medidas de corrección inmediatas desde el gráfico/ árbol de procesos de incidentes activando un flujo de trabajo SOAR por demanda esto puede ser: Aislamiento de dispositivos, bloqueo de autenticación de usuarios, deshabilitación de usuarios, envío de artefactos al sandboxing, captura de datos de análisis forense, entre otros los cuales pueden ser personalizados o creados de acuerdo a las necesidades	x		Se verifica el cumplimiento en la ficha técnica del producto
147	- La plataforma debe contar con un BOT que tenga el rol de analista de ciberseguridad que apoye los equipos de investigación, cacería de amenazas y administradores de seguridad para poder acelerar las actividades de su día a día. - El BOT debe simplificar el proceso de determinar riesgos y actividad maliciosa en el entorno y reducir la necesidad de revisar y filtrar manualmente grandes cantidades de datos. Puede generar avisos o registros de avisos para determinar rápidamente qué adversarios se han detectado en la organización o han atacado a otras organizaciones del sector, encontrar endpoints afectados por vulnerabilidades de alto riesgo y mucho más. - La interacción con el BOT debe ser por medio del establecimiento de conversaciones introduciendo una consulta en la barra de conversaciones o ejecutando un libro de indicaciones (conjunto de preguntas), la plataforma debe mantener el contexto de varias preguntas para llegar a la respuesta. la información consultada debe corresponder únicamente a los datos alojados por la plataforma y sus módulos activos únicamente.	x		Se verifica el cumplimiento en la ficha técnica del producto
148	Las respuestas se deben generar en el orden en que las solicitudes se encuentran en la cola. El formato y la cantidad de información de una respuesta pueden variar según la solicitud. De acuerdo a las consultas deben incluir en su mayoría tablas de resultados y un resumen general que los describe, con un concepto de seguridad y análisis. Según los datos de la tabla, puede copiar los datos JSON generados o descargar un CSV, si está disponible. Siempre utilizando lenguaje natural	x		Se verifica el cumplimiento en la ficha técnica del producto
149	El analista BOT debe tener integraciones con el sistema para tener un uso adicional para: - Crear y correr consultas (queries) sobre los datos y datos crudos recopilados sobre la plataforma.	x		Se verifica el cumplimiento en la ficha técnica del producto

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	- Analizar líneas de comando ejecutados en las cargas de trabajo sin límite de uso: Esto es decodificar, desofuscar y explicar el propósito de una línea de comando o script que se capture en una detección de EDR (ej. Comandos vía powershell). - Crear diagnósticos de detecciones indicando un Score de evaluación de impacto vía AI, explicando porque puede ser potencialmente peligroso y teniendo un concepto para acelerar el proceso de diagnóstico de detecciones, esto por medio del uso de lenguaje natural			
150	La capacidad de que el analista BOT haga el diagnóstico de detecciones (triage) debe presentar un tablero de control que muestre en un rango de tiempo desde 1 hora, un dia, una semana, 30 días, o 90 días: - Cantidad total de diagnósticos y diagnóstico en el tiempo. - Tiempo promedio que toma hacer los diagnósticos. - Tiempo ahorrado en esta actividad. - Detecciones más recientes. - Cantidad de veredictos realizados: Verdaderos positivos, Falsos positivos o sin veredicto	x		Se verifica el cumplimiento en la ficha técnica del producto
151	El consumo de este servicio de BOT debe basar en el número de consultas ejecutadas por mes con el objetivo de tener una consulta de su consumo, teniendo en cuenta que si se realiza una consulta que se ha realizado en los últimos 30 días la plataforma no debe considerarlo una nueva consulta ejecutada	x		Se verifica el cumplimiento en la ficha técnica del producto
	SERVICIO DE SOPORTE Y GARANTÍA TÉCNICA			
152	SOPORTE DEL FABRICANTE: El fabricante debe brindar un soporte en horario de 24x7 (Las 24 horas del día, los 7 días a la semana) desde la firma del contrato, por una vigencia de 24 meses. - Acceso al portal de soporte (base de conocimiento, Escalamiento de Tickets). - 7x24x365 soporte telefónico. - Priorización de Caso. - Asignación de un TAM (especialista de producto) para revisión y evaluación periódica. - Healthcheck de la solución de forma trimestral. - Reportes trimestrales. - Gestión de casos proactivos. - Acompañamiento en nuevas funcionalidades y actualizaciones. - Acompañamiento en el Kick Off del proyecto.	x		Cumple y se anexa certificado de sopoirte y garantía técnica
153	Tiempos de respuesta: El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el supervisor del contrato. - Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente. - De ser necesario el proveedor deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas. - El tiempo máximo permitido para restablecer el servicio es de 4 horas	x		Cumple y se anexa certificado de sopoirte y garantía técnica
154	Tipo De Atención: - Soporte Nivel 1: De manera presencial dos días a la semana con duración de 8 horas laborales (2x8) en las instalaciones del Comando General de las Fuerzas Militares Centro Administrativo Nacional CAN edificio Fortaleza Carrera 54 # 26-25 en la ciudad de Bogotá, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato. - Soporte Nivel 2: Cuando se requiera por medio telefónico o de manera remota a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato, y de acuerdo con los términos y tiempos de respuesta especificados.	x		Cumple y se anexa certificado de sopoirte y garantía técnica
155	GARANTIA DE SOPORTE - El Contratista deberá garantizar el normal funcionamiento después de la implementación y puesta en marcha de la solución, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. - Soporte disponible los 365 días del año en horario 7x24 (7 días a la semana las 24 horas del día). - El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica gratuita, servicio de correo electrónico o en forma remota de acuerdo a los niveles de servicio. En un lapso de cuatro (04) horas después de haber reportado el	x		Cumple y se anexa certificado de sopoirte y garantía técnica

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas.			
156	El proponente debe integrar a su propuesta los siguientes servicios: - Servicio por parte del fabricante para poder hacer al menos 02 workshops durante el despliegue de la plataforma (Taller de buenas prácticas de despliegue y análisis de detecciones para una correcta comprensión). - Servicio de asignación de un TAM - Tecnical account manager por parte del fabricante para que realice una evaluación continua de la configuración de la plataforma y apoyo en la gestión de casos de soporte cuando se hace el escalamiento con fábrica. - Se debe tener acceso a entrenamientos en línea por parte del fabricante sin límite para los funcionarios de la entidad durante la vigencia del contrato.	x		Cumple y se anexa certificado de sopoirte y garantia técnica
	TRASFERENCIA DE CONOCIMIENTO			
157	El Contratista debe realizar transferencia de conocimiento para el personal que administra la solución, de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica	X		Se realizo la transferencia de conocimiento y se anexan los soportes
158	Debe incluir material técnico, en la ciudad de Bogotá en Idioma español; se debe ofrecer una metodología teórica y práctica con laboratorios de cómputo debidamente configurados, en instalaciones dispuestas por el contratista que incluya equipos de cómputo, material impreso, digital, de software y hardware	X		Se realizo la transferencia de conocimiento y se anexan los soportes
159	El contratista debe disponer de aulas completamente dotadas que cubran todos los aspectos logísticos para la ejecución de los entrenamientos requeridos, igualmente proveer instructores idóneos, calificados y certificados, con experiencia en la ejecución de capacitación	X		Se realizo la transferencia de conocimiento y se anexan los soportes
160	El Contratista deberá entregar el material de clases necesario para desarrollar el entrenamiento de acuerdo a cada uno de los módulos. Así mismo, se deberán entregar las presentaciones utilizadas por los instructores	X		Se realizo la transferencia de conocimiento y se anexan los soportes
161	El Contratista deberá emitir un certificado a cada uno de los estudiantes que aprueben la transferencia tecnológica	X		Se realizo la transferencia de conocimiento y se anexan los soportes
162	LA CAPACITACIÓN DEBERÁ ESTAR ENFOCADA EN: - Configurar la solución la solución adquirir. - Crear políticas para la protección dentro de la organización. - Gestión de hosts. - Respuesta de incidentes. - Caza de Amenazas. - Despliegue del Agente. - Protección de datos. - Detención y respuesta EDR-XDR. - Antivirus y Antimalware.	X		Se realizo la transferencia de conocimiento y se anexan los soportes
163	El objetivo de esta transferencia de conocimiento es capacitar al personal de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares para que puedan gestionar, instalar, configurar y analizar los productos adquiridos de manera efectiva y adecuada. El certificado emitido por el fabricante y/o distribuidor autorizado servirá como evidencia de la participación y aprobación de la capacitación por parte de los funcionarios	X		Se realizo la transferencia de conocimiento y se anexan los soportes
	CONFIDENCIALIDAD DE LA INFORMACIÓN			
164	El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción "acuerdo de confidencialidad"	x		Se anexa el acuerdo de confidencialidad
165	La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal	x		Se anexa el acuerdo de confidencialidad

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización			
166	A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este Item. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento	x		Se anexa el acuerdo de confidencialidad
167	Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros	x		El contratista se compromete a cumplir las políticas de seguridad informática del Comando General
168	El contratista y los recursos humanos que formarán parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el acuerdo de confidencialidad donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros	x		El contratista se compromete a cumplir las políticas de seguridad informática del Comando General
	CRONOGRAMA			
169	Dentro de los primeros cinco (05) días calendario del plazo de ejecución, el contratista deberá presentar el cronograma para la ejecución del objeto del contrato, para aprobación del supervisor del contrato, que incluya el proceso y actividades de: - Planeación (requerimientos y preparación) - Despliegue (Posibles esquemas de despliegue de sensores, como puede acelerar el proceso), proceso de implementación para minimizar la fricción o interrupciones con la plataforma actual. - Post-Implementación (se debe indicar como es el proceso de escalamiento de nuevos requerimientos, atención de solicitudes de soporte - portales/teléfono/equipo encargado, apoyo en la revisión del estado de la plataforma como informar las nuevas funcionalidades que son importantes incorporar, durante la ejecución del contrato).	x		Se aprueba el cronograma de ejecución
	SERVICIO DE INGENIERA SOPORTE E IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DE LA SOLUCIÓN DE ACUERDO A DOCUMENTO DE ESPECIFICACIONES TÉCNICAS			
	Implementación del Proyecto			
170	El contratista junto con el supervisor del contrato debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con la seguridad perimetral	x		Se verifica el contrato y el cronograma de trabajo se realiza y aprueba de acuerdo al análisis de las especificaciones tecnicas
171	El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones	x		El personal que participa en el proyecto tiene las capacidades tenicas
172	Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Comando General de las Fuerzas Militares	x		Se realiza la instalación y configuración, los que se evidencia en el informe de instalación que reposa en el computador del administrador por contener información de seguridad
173	El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Comando General que sean necesarias para el óptimo funcionamiento de todas las tecnologías	x		No se generaron costos adicionales para la institucion

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
174	El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de la solución a adquirir con sus correspondientes integraciones, con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Comando General de las Fuerzas Militares	x		El diagrama de la solución e información tecnica se encuentra el la carpeta c://edr del computador del administracion de la plataforma
175	Las soluciones a implementar deben ser compatibles con las plataformas actuales del Comando General y cumplir con el protocolo IPv4 e IPV6	x		Cumple de acuerdo a la especificación tecnica
176	Toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato	x		En la implementación no se presentaron indisponibilidades derivadas de la ejecución del proyecto
177	Caso de Fallas: - Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. - En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo: * Implementación de software. * Configuraciones, puesta en producción y funcionamiento.	x		No se presentaron fallas en la ejecución del contrato
	Integración			
178	Realizar una correcta implementación: Es importante realizar una correcta implementación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware y software.	x		Se realiza la instalación y configuración, los que se evidencia en el informe de instalación que reposa en el computador del administrador por contener información de seguridad
179	Configuración adecuada: La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red	x		Se realiza la instalación y configuración, los que se evidencia en el informe de instalación que reposa en el computador del administrador por contener información de seguridad
180	Pruebas de integración: El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.	x		Se realiza la instalación y configuración, los que se evidencia en el informe de instalación que reposa en el computador del administrador por contener información de seguridad
	Herramienta o software de implementación y despliegue masivo de agentes			
181	Deberá suministrarse una herramienta licenciada para el proceso de implementación de la solución que permita automatizar la instalación, actualización y desinstalación de los agentes en múltiples equipos de cómputo al mismo tiempo que cumpla con las siguientes especificaciones: - Descubrimiento de activos: Acceder fácilmente a los datos de sus dispositivos locales, incluidas las versiones de software antiguas. - Sincronización automática con AD: Sincronizar con Active Directory para importar registros de computadoras automáticamente. - Se requiere de un software que se pueda instalar en cualquier dispositivo PC o servidor Windows para poder realizar procesos de despliegue masivos de software. No debe requerir un servidor dedicado y puede ser también desplegado de forma distribuida para mayores capacidades de despliegue. - Este software debe ser de un fabricante independiente. - La herramienta de despliegue debe poder realizar identificación de dispositivos como: * Dispositivos pertenecientes al directorio activo, donde se pueda definir cuentas de administración generales o parciales para hacer despliegues de software, como también selección granular de dispositivos objetivo como grupos del directorio activo. * Dispositivos windows donde se puede hacer despliegues vía powershell por medio de scripts.	x		Se realiza la implementación de la herramienta de despliegue

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	* Dispositivos linux donde se pueden hacer despliegues via SSH por medio de scripts * Listas de dispositivos por medio de la importación de listados. - La herramienta de despliegue debe tener la capacidad de personalizar tareas y paquetes para poder lanzar tareas en paralelo sin afectar despliegues anteriores. - La herramienta de despliegue debe permitir un seguimiento detallado del proceso de despliegue indicando errores en el proceso para poder remediar de forma adecuada			
182	ESTUDIO DE SEGURIDAD PERSONAL: El contratista debe aceptar y permitir que el COGFM efectúe un Estudio de Seguridad Personal (ESP) a los funcionarios designados para el desarrollo del proyecto, a fin de comprobar datos y establecer antecedentes disciplinarios; que garanticen la seguridad de la información. Los formatos de seguridad personal (ESP), deberán ser entregados al supervisor del contrato, debidamente diligenciados a más tardar pasados 15 días calendario de la firma y perfeccionamiento del contrato, cuando ello hubiere lugar	x		Se realiza el esp del personal y se anexa oficio enviándolo a J2
183	El contrato debe ejecutarse a todo costo, el contratista se compromete a prestar el servicio con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad	x		No se generaron sobre costos en la ejecución del contrato
184	El contratista deberá garantizar el personal suficiente, idóneo con profesionales calificados necesarios para la completa ejecución y cumplimiento del contrato, sin que esto genere costo adicional para el Comando General de las Fuerzas Militares, de igual manera disponga de instalaciones y equipos de cómputo propias para la ejecución del proyecto	x		Se verifica el cumplimiento del personal que participa en el proyecto
185	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia, en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se realiza la lectura de las especificaciones técnicas del contrato
186	El Comando General de las Fuerzas Militares no asumirá ninguna responsabilidad contractual ni laboral con los funcionarios que la empresa contratista asigne para el cumplimiento del contrato	x		El personal que participa se encuentra a cargo de la empresa
187	PERSONAL PARA LA EJECUCIÓN DEL CONTRATO - GERENTE DE PROYECTO: RONALD ALEXANDER CASTAÑEDA OLARTE, Ingeniero electrónico - INGENIERO IMPLEMENTADOR: EDGAR ALFONSO GODOY LOPEZ, Ingeniero de Sistemas	x		Se anexan las planillas de seguridad social del personal
188	En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario. Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa	x		No se realizaron cambios de personal
189	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto	x		No se realizaron cambios de personal
190	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado	x		Se verifican las planillas de pago de seguridad social y se anexa copia
191	El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente	x		No se realizaron cambios de personal

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato			
192	Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		El contratista acepta los términos del contrato
193	El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato	x		El contratista cumple con las normas de seguridad industrial
194	El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma	x		El personal comprometido en la ejecución del contrato esta a cargo de contratista
	LOTE 5: SUSCRIPCIÓN WAF			
195	La solución de seguridad deberá proporcionar una plataforma unificada de seguridad que integre servicios de protección contra ataques de denegación de servicios distribuida, firewall de aplicaciones web (WAF), seguridad para APIs y detección y prevención de bots maliciosos y usuarios reales comprometidos	x		La solución cumple de acuerdo a la ficha tecnica
197	La solución de seguridad deberá ofrecer estos servicios en la nube del fabricante no se aceptarán despliegues en nube pública	x		La solución cumple de acuerdo a la ficha tecnica
198	La solución de seguridad deberá incluir al menos dos balanceadores de carga, cada uno con soporte para un mínimo de 32 aplicaciones web, y al menos dos direcciones IP ANYCAST distribuidas en todos los centros de datos de la solución de seguridad para la publicación de los servicios web de la entidad. Estas aplicaciones podrán estar asociadas a un mínimo de 200 nombres de dominio raíz diferentes	x		La solución cumple de acuerdo a la ficha tecnica
199	La solución de seguridad deberá realizar el enforcement de políticas de seguridad para las aplicaciones WEB y APIs, tanto en los nodos regionales o puntos de presencia, como en los múltiples proveedores de nube o en las premisas	x		La solución cumple de acuerdo a la ficha tecnica
200	Esta solución de seguridad deberá contar con soporte y garantía por parte del fabricante. La vigencia de la suscripción soporte y garantía deberá ser de dos (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante	x		La solución cumple de acuerdo a la ficha tecnica
	CARACTERÍSTICAS TÉCNICAS			
201	SaaS - La solución deberá soportar una arquitectura Software as a Servicie (SaaS), donde la manera de consumo de los servicios sea dentro de su propio cloud, incluyendo todos los puntos de presencia distribuidos de manera global. - La solución deberá ofrecer disponibilidad de ancho de banda limpio en su servicio WAF o protección de aplicaciones web, sin limitación en el volumen de datos por solicitud inspeccionada o mitigada, garantizando la protección para todo el tráfico que llegue a la Entidad, hasta un máximo de treinta (30) millones de requests mensuales como parámetro de dimensionamiento y control operativo. - La solución deberá incluir al menos dos balanceadores de carga, cada uno con soporte para un mínimo de 32 aplicaciones web, y al menos dos direcciones IP ANYCAST distribuidas en todos los centros de datos de la solución para la publicación de los servicios web de la entidad. Estas aplicaciones podrán estar asociadas a un mínimo de 200 nombres de dominio raíz diferentes.	x		La solución cumple de acuerdo a la ficha tecnica
	ADMINISTRACIÓN			
202	Gestor Centralizado / Consola Central La solución deberá proporcionar una consola central SaaS para la administración centralizada de las configuraciones de red y seguridad, así como también acceso a herramientas de troubleshooting y dashboard donde se visualice la disponibilidad y el estado de los servicios. Además, debe permitir que la gestión se realice mediante clickops, API requests, Terraform o integrandose al pipeline CI/CD de la organización	x		La solución cumple de acuerdo a la ficha tecnica
203	API de la solución La solución deberá ser full RESTful-API o API first: - Permitiendo realizar todas las configuraciones a través de su API, así como también, la petición de información de los dashboards.	x		La solución cumple de acuerdo a la ficha tecnica

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	- Debe estar bien documentada y proveer de las configuraciones en JSON y YAML de cualquiera de los objetos que se definan. - Debe permitir la creación de credenciales por usuario, el uso de API token, certificados, así como la creación de usuarios API con RBAC.			
204	Usuarios Admin La solución deberá soportar la creación de múltiples usuarios, así como roles de acceso como read only, SecOps, DevOps, NetOps, SuperUser, Billing User entre otros.	x		La solución cumple de acuerdo a la ficha técnica
205	RBAC La solución deberá permitir el uso de RBAC para el control de acceso de los usuarios al gestor centralizado, permitiendo la delimitación de las APIs/recursos que se pueden visualizar y/o administrar.	x		La solución cumple de acuerdo a la ficha técnica
206	Self Service La solución deberá proporcionar al usuario del gestor centralizado la posibilidad de administrar sus servicios dentro de una consola unificada y donde se permita la colaboración de distintos equipos (SecOps,DevOps,entre otros)	x		La solución cumple de acuerdo a la ficha técnica
207	Servicio Administrado La solución deberá contemplar la opción de incluir un servicio administrado para WAAP, operado por personal especializado y certificado por el fabricante, el cual será presentado como un componente opcional y evaluado de forma independiente a la solución principal	x		La solución cumple de acuerdo a la ficha técnica
208	Soporte La solución deberá contar con soporte 24x7, ya sea por medio de Teléfono, Mail u otros medios de contacto. Asimismo, el servicio de soporte deberá permitir la interacción con el Centro de Soporte en idioma español en el uso horario de la región (Colombia) durante horario laboral.	x		La solución cumple de acuerdo a la ficha técnica
209	Capacitación La solución deberá contar con capacitación onDemand a través de videos y/o documentación que ejemplifiquen configuraciones básicas y que sean accesible desde la plataforma o página web del fabricante	x		La solución cumple de acuerdo a la ficha técnica
	VISIBILIDAD			
210	Integración con SIEM La solución deberá proporcionar integración con herramientas de logging de terceros.	x		La solución cumple de acuerdo a la ficha técnica
211	Dashboard de Performance La solución SaaS deberá proporcionar visibilidad acerca de: - Salud de la aplicación - Alertas activas - Origin Servers/Backends - Latencia de fin a fin - Visitantes únicos - Tipo de dispositivo - Peticiones (Request Rate, Total Request, Error rate, total errors, drop rate, drop count) - Throughput - ASN - TLS Fingerprint - TLS Ciphers y protocolos - Códigos de error de HTTP - Localización de clientes - Top URLs	x		La solución cumple de acuerdo a la ficha técnica
212	Dashboard de Seguridad La plataforma SaaS deberá proporcionar visibilidad sobre: - Eventos de seguridad por aplicación (WAF, APISec, DDoS, Anti-Bot entre otros) - Top ten de las firmas con más hits - Eventos localizados geográficamente - Tipos de ataques - Score de usuarios maliciosos - Clasificación de bots (humano, malicioso, Sospechoso) Asimismo, la solución deberá proporcionar filtros para búsquedas utilizando el identificador asociado con el evento de seguridad.	x		La solución cumple de acuerdo a la ficha técnica
213	Auditoria La plataforma SaaS deberá proporcionar visibilidad sobre los cambios de	x		La solución cumple de acuerdo a la ficha técnica

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	configuración realizados por los usuarios del gestor centralizado durante un periodo de tiempo de 30 días			
	CERTIFICACIONES			
214	- California Consumer Privacy Act (CCPA): Deberá estar en cumplimiento con lo dispuesto por California Consumer Privacy Act (CCPA) - General Data Protection Regulation (GDPR): Deberá estar en cumplimiento con lo dispuesto por General Data Protection Regulation (GDPR) - System and Organization Controls (SOC) Type 2: La solución deberá contar con la certificación System and Organization Controls (SOC) Type 2	x		Cumple de acuerdo a la ficha técnica de la solución
	SLAs	x		Cumple de acuerdo a la ficha técnica de la solución
215	- Disponibilidad: La plataforma SaaS deberá proporcionar un 99.99% de disponibilidad - Tiempo de Respuesta: El servicio de Soporte técnico de la solución propuesta deberá tener un tiempo de respuesta de 30min para el primer contacto - Analisis de Causa Raiz: El servicio de Soporte técnico de la solución debe cumplir con el siguiente SLA relacionado con el análisis de causa raíz de un incidente: * Incidente de severidad crítica: proporcionar un draft a las 24 hrs y el análisis final en 7 días			Cumple de acuerdo a la ficha técnica de la solución
	WEB SECURITY			
216	Web Application & API Security - La solución propuesta deberá emplear una combinación de técnicas algorítmicas, basadas en firmas, utilización de bases reputacionales y machine learning para identificar ataques a nivel de aplicación y API, proporcionando una solución holística de firewall aplicativo de próxima generación. - La solución deberá contar con un motor de machine learning para determinar de manera automática todos los API endpoints que son accedidos a través de cualquiera de los servicios virtuales publicados. Además, deberá permitir que la información aprendida pueda ser utilizada para la definición de políticas por aplicación	x		Cumple de acuerdo a la ficha técnica de la solución
217	Web Application Firewall: La solución deberá proporcionar una plataforma SaaS con motor de Machine Learning y firmas para la detección de ataques a nivel de capa de aplicación, que incluya la detección de ataques del OWASP TOP 10 así como los últimos ataques conocidos con actualización automática en valores de firmas, así como la utilización de una base de datos asistida de campanas de amenazas para detección de ataques específicos alrededor del mundo.	x		Cumple de acuerdo a la ficha técnica de la solución
218	Detección de Usuarios Maliciosos: La solución deberá contar con la capacidad de detectar usuarios maliciosos mediante el análisis de su comportamiento utilizando técnicas y modelos avanzados, tal como Machine Learning.	x		Cumple de acuerdo a la ficha técnica de la solución
219	Supresión de falsos positivos: La solución deberá utilizar un modelo de Machine Learning para el perfilamiento del tráfico dentro del WAF que permita la supresión de falsos positivos.	x		Cumple de acuerdo a la ficha técnica de la solución
220	Tuning de la base de firmas: La solución deberá contar con un mecanismo automático que permita el tuning de las firmas de ataques	x		Cumple de acuerdo a la ficha técnica de la solución
221	DDoS L3/L4: La solución deberá contar con la capacidad de detección y mitigación automática de ataques volumétricos de denegación de servicio, sin límite en la cantidad de este tipo de eventos y sin ancho de banda mínimo para la mitigación.	x		Cumple de acuerdo a la ficha técnica de la solución
222	DDoS L7: La solución deberá permitir el bloqueo de clientes/usuarios de la aplicación basándose en su comportamiento. La solución deberá permitir la definición de políticas de retos de identificación de usuario de la aplicación utilizando JavaScript y CAPTCHA	x		Cumple de acuerdo a la ficha técnica de la solución
223	Antibot: La solución deberá contar con la funcionalidad de Anti-Bot permitiendo la categorización de bots en buenos, sospechosos y malos y, por ende, su mitigación.	x		Cumple de acuerdo a la ficha técnica de la solución
224	Servicio de reputación de IP: La solución deberá contar con la funcionalidad de bloqueo automático de conexiones desde IPs consideradas maliciosas, mediante la utilización de una base dinámica de reputación de IPs.	x		Cumple de acuerdo a la ficha técnica de la solución

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
225	Bloqueo de peticiones no deseadas: La solución deberá permitir el bloqueo de clientes basándose en su comportamiento, el ASN, la red, la dirección IP y el país desde donde se generó la conexión	x		Cumple de acuerdo a la ficha técnica de la solución
226	Cifrado: La solución deberá permitir la configuración de Cifrados de acuerdo a diferentes perfiles: alto, medio o bajo, así como la creación de políticas personalizadas para utilización de ciphers y protocolos específicos por aplicación. High: - TLS 1.2 y 1.3 TLS_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	x		Cumple de acuerdo a la ficha técnica de la solución
227	Generación Automática de Certificados Digitales: La solución deberá permitir la configuración de certificados públicos firmados de manera automática y controlados de manera automática a través de alguna delegación de dominio o validación de registros de DNS	x		Cumple de acuerdo a la ficha técnica de la solución
228	Reescrituras HTTP: La solución deberá permitir la configuración de reescrituras HTTP. Asimismo, deberá permitir el tratamiento tanto de las peticiones HTTP hacia las aplicaciones, como de respuestas personalizadas según los diferentes códigos de HTTP.	x		Cumple de acuerdo a la ficha técnica de la solución
229	Balanceo de cargas: La solución deberá permitir la configuración de origen servers/backend servers y sus correspondientes monitores de salud de manera ilimitada. Asimismo, la solución deberá permitir el uso de los siguientes métodos de balanceo: - RoundRobin - Least Active Request - Random - Persistencia por dirección IP - Persistencia basada en cookie - Ring Hash Así como crear pesos sobre los orígenes que se deseen y asignar esquemas activo-pasivo.	x		Cumple de acuerdo a la ficha técnica de la solución
239	Analítica de Comportamiento de Usuario: La solución deberá contar con mecanismos que permitan el análisis de comportamiento utilizando métricas y logs. El análisis de comportamiento debe incluir: - Detección de anomalías por petición, utilizando métricas como tamaño de la petición, tamaño de la respuesta, latencia. -Lógica de Negocio, utilizando los logs de peticiones, por cliente por servidor y el host virtual para aprender: elementos dinámicos, probabilidad de función, tiempos y anomalías analiza esto utilizando redes neuronales.	x		Cumple de acuerdo a la ficha técnica de la solución
231	Control sobre el número de peticiones (Rate Limit L7 DoS): La solución deberá permitir controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre API endpoints específicos.	x		Cumple de acuerdo a la ficha técnica de la solución
232	CSRF: La solución deberá controlar los subdominios permitidos en las peticiones cruzadas dentro de un Load Balancer/Proxy	x		Cumple de acuerdo a la ficha técnica de la solución
233	Manejo de Información sensible: La solución deberá permitir controlar la información a visualizar de las respuestas del servidor, permitiendo enmascarar la información considerada como sensible, como, por ejemplo: datos de tarjeta de crédito	x		Cumple de acuerdo a la ficha técnica de la solución
234	Client Side Defense: La solución debe proveer de un sistema de protección multifase a las aplicaciones Web, contra Formjacking, Magecart-style, y otros ataques de JavaScript. La protección multifase debe incluir detección, alertamiento y mitigación	x		Cumple de acuerdo a la ficha técnica de la solución
235	Identificación del usuario: La solución deberá identificar usuarios teniendo en consideración los siguientes parámetros: ClientIP, TLSFingerprint, Cookie, HTTP Header, Client ASN, Client City, Client Region, Query Parameter Key.	x		Cumple de acuerdo a la ficha técnica de la solución
236	Engine de WAF unificado: La solución deberá utilizar el mismo motor de WAF cualquiera sea la arquitectura implementada: SaaS, On-Premise, Hibrido,	x		Cumple de acuerdo a la ficha técnica de la solución

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	permitiendo la extensión de las políticas o servicios de seguridad a los diferentes ambientes que la constituyen.			
237	Mutual TLS: La solución deberá permitir la utilización de MTLS para comunicación hacia los clientes y hacia los servidores.	x		Cumple de acuerdo a la ficha técnica de la solución
238	Cookie Protection: La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticacion.	x		Cumple de acuerdo a la ficha técnica de la solución
239	GraphQL Inspection: La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando instrospeccion, de los recursos, disponibles en el esquema actual.	x		Cumple de acuerdo a la ficha técnica de la solución
240	Ruteo de requests HTTP: La solución deberá permitir la redirección de peticiones a distintos grupos de origen servers/backend servers dependiendo de: - Prefijo de URI - HTTP header - Cookie - Método HTTP aplicando reglas de WAF por cada ruta, así como reglas de seguridad específicas.	x		Cumple de acuerdo a la ficha técnica de la solución
241	Mitigación de Usuarios Maliciosos: La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos: low, medium, high. Dependiendo del puntaje por los eventos de seguridad de un usuario, la solución debe contar con la capacidad de mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.	x		Cumple de acuerdo a la ficha técnica de la solución
242	Errores de Respuesta Personalizados: La solución deberá permitir crear un mensaje de respuesta personalizado por cada código de error HTTP	x		Cumple de acuerdo a la ficha técnica de la solución
243	Tamaño de los headers: La solución deberá permitir limitar el tamaño de los headers HTTP de los requests/peticiones de los usuarios	x		Cumple de acuerdo a la ficha técnica de la solución
244	Manipulación de Headers: La solución deberá permitir la eliminación o adición de nuevos headers HTTP en las respuestas o peticiones entre el cliente y servidor. Por ejemplo: la solución deberá ser capaz de insertar el header X-Forwarded-For HTTP Header para informar al origen server/backend server de la dirección IP original del request del cliente	x		Cumple de acuerdo a la ficha técnica de la solución
245	CORS: La solución deberá tener la capacidad de proteger contra CORS	x		Cumple de acuerdo a la ficha técnica de la solución
246	GeoIP protection: La solución deberá permitir el control de acceso de los usuarios a la aplicación según el país de origen, permitiendo reglas de allow o deny desde países en específico; por ejemplo: que se permita el acceso solo a un país, y se bloquee el resto.	x		Cumple de acuerdo a la ficha técnica de la solución
247	Service Policies: La solución deberá permitir la creación de reglas de L3, L7 para permitir o negar el acceso a recursos, así como el manejo de los diferentes motores de seguridad para la creación de excepciones.	x		Cumple de acuerdo a la ficha técnica de la solución
248	Protección contra ataques sofisticados o campañas activas: La solución deberá contar con la capacidad de proteger a las aplicaciones contra ataques sofisticados o ataques "In-the-wild" con gran precisión, de manera que la información contextual de esos ataques reales utilizados alrededor del mundo sea empleada para la creación de firmas de WAF en tiempo real.	x		Cumple de acuerdo a la ficha técnica de la solución
	API Security	x		Cumple de acuerdo a la ficha técnica de la solución
249	Monitoreo y Protección de APIs: La solución deberá tener la capacidad de monitorear y proteger las APIs tan cerca del origen como sea posible. Además, la solución debe brindar esta capacidad utilizando el mismo motor de protección tanto en el propio cloud, como en clouds públicos/privados y en las premisas.	x		Cumple de acuerdo a la ficha técnica de la solución
250	API Anomaly Detection: La solución deberá contar con un mecanismo de análisis de comportamiento de las peticiones/request hacia cualquier de los API endpoints definidos, permitiendo la detección de anomalías por petición/request.	x		Cumple de acuerdo a la ficha técnica de la solución
251	API Discovery: La solución deberá contar con la capacidad de aprender/determinar los API endpoints que son accedidos, incluyendo petición y respuesta, y detectar información sensible. Además, debe proveer la vista de API endpoints en inventario,	x		Cumple de acuerdo a la ficha técnica de la solución

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	shadow y descubiertas, y generar un Probability Distribution Function (PDF) para las métricas relacionadas a cada endpoint, con actualización periódica. Esta funcionalidad aplicará para un (1) API, con un máximo de quinientos mil (500.000) requests mensuales en protección.			
252	Sensitive Data: La solución deberá contar con la capacidad de identificar y localizar la información sensible en las peticiones desde los clients y en las respuestas de los API endpoints. Deberá identificar PII, tal como números de tarjeta de crédito y numero de seguridad social e indicar el parámetro/campo donde la información esta localizada.	x		Cumple de acuerdo a la ficha técnica de la solución
253	API Endpoint Learning: La solución deberá contar con un mecanismo que permita el descubrimiento dinámico de las APIs, determinar cuáles endpoints deberían ser utilizados y permitir únicamente estos API endpoints, obtener información de la utilización, como tamaño de las peticiones y frecuencia. Asimismo, la solución deberá proporcionar las siguientes métricas: tamaño de la petición/respuesta, latencia con datos y latencia sin datos, frecuencia de peticiones, frecuencia de errores, troughput de las respuestas.	x		Cumple de acuerdo a la ficha técnica de la solución
254	API Schema Learning: La solución deberá aprender la estructura del esquema de las APIs, analizando los requests/peticiones y respuestas para cada una de ellas. Asimismo, deberá permitir la descarga del swagger file aprendido.	x		Cumple de acuerdo a la ficha técnica de la solución
255	Importación de especificación (Swagger file): La solución deberá permitir la importación de las especificaciones del API contenidas en un archivo Swagger.	x		Cumple de acuerdo a la ficha técnica de la solución
256	API Authentication Discovery: La solución debe contener sensores integrados para la detección de tipos de autenticación, y localización en las llamadas API. Una vez detectados, se deben asociar con un edpoint y mostrar un estado de autenticación.	x		Cumple de acuerdo a la ficha técnica de la solución
257	JSON Web Token Discovery: La solución deberá ser capaz de descubrir el header, payload y firma de JWTs así como la identificación de campos utiles para el cliente, permitiendo la identificación de datos sensibles en los payloads de JWT así como la definición del score de riesgo.	x		Cumple de acuerdo a la ficha técnica de la solución
258	Detección de Usuarios Maliciosos: La solución debe contar con un motor de WAF que permita realizar un perfilamiento de usuarios, utilizando: la cantidad de firmas identificadas, cantidad de accesos prohibidos, errores de login, tasa de errores.	x		Cumple de acuerdo a la ficha técnica de la solución
259	Mitigación de Usuarios Maliciosos: La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos, low, medium, high y dependiendo del puntaje por los eventos de seguridad de un usuario, realizar una mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.	x		Cumple de acuerdo a la ficha técnica de la solución
260	Control sobre el número de peticiones Rate Limit L7: La solución deberá controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre endpoints específicos.	x		Cumple de acuerdo a la ficha técnica de la solución
261	API Security: La solución deberá permitir la carga de archivos Swagger para cada versión de la API, controlando el modo de consumo de los endpoints por frecuencia o método HTTP. Donde todo lo que no se encuentra dentro de la definición de Open API (swagger file) (o explícitamente permitido) sea bloqueado. La solución deberá permitir la creación de políticas de seguridad, donde se contemplen excepciones que permitan el acceso a usuarios específicos dentro de API end points o grupos de API.	x		Cumple de acuerdo a la ficha técnica de la solución
262	Manejo versionamiento de definición de APIs: La solución deberá permitir la carga de distintos archivos Swagger, dependiendo de la versión de la API a proteger, y añadir la definición en distintos segmentos dentro del balanceador.	x		Cumple de acuerdo a la ficha técnica de la solución
263	Cookie Protección: La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticación.	x		Cumple de acuerdo a la ficha técnica de la solución
264	GraphQL Inspection: La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando introspección, de los recursos, disponibles en el esquema actual.	x		Cumple de acuerdo a la ficha técnica de la solución
265	API Discovery - La solución debe disponer de una función de descubrimiento de API que lea e identifique los API endpoints en el repositorio de código.	x		Cumple de acuerdo a la ficha técnica de la solución

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	- La solución debe tener una función de descubrimiento de API que lea e identifique los puntos finales de API de dominios externos, rastreando los dominios externos.			
	HERRAMIENTA DE PENTEST AUTOMATIZADA	x		
266	Prueba de penetración automatizada: La solución debe contar con una solución Dynamic Application Security Testing(DAST) en la nube para aplicaciones web y API. La prueba de penetración puede configurarse en minutos y solo requiere la URL de su aplicación web/API junto con las credenciales de uno o más usuarios de prueba que pueden utilizar para iniciar sesión en su aplicación de destino automáticamente.	x		Cumple de acuerdo a la ficha técnica de la solución
267	Tipo de vulnerabilidades: El servicio Scan debe identificar vulnerabilidades en sus aplicaciones web y APIs. Estas pruebas se basan en el OWASP Top 10, un documento de concienciación estándar para desarrolladores y seguridad de aplicaciones web. El servicio Scan también debe incluir pruebas propias y pruebas curadas por la comunidad. Estas son algunas de las pruebas que debería realizar Scan: - Broken Access Control - Business Logic Attacks - SQL Injection (incl. Blind SQL Injection): - Cross-Site Request Forgery (CSRF): - Cross-Site Scripting (XSS) (Stored, Reflected, DOM-based) - Insecure Direct Object References (IDOR) - Security Misconfiguration - Vulnerable and Outdated Components - Identification and Authentication Failures - Software and Data Integrity Failures - Security Logging and Monitoring Failures - Server-Side Request Forgery (SSRF)	x		Cumple de acuerdo a la ficha técnica de la solución
268	Tipos de servicios: La solución de seguridad debe realizar scans y servicios de recon.	x		Cumple de acuerdo a la ficha técnica de la solución
	GARANTÍA TÉCNICA Y SERVICIO			
269	Garantizar soporte del fabricante 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante. El soporte del fabricante deberá incluir: - Soporte vía correo electrónico - Soporte vía telefónica - Recepción de alertas, mensajes o noticias sobre las actualizaciones del servicio durante el periodo contratado. - Ningún límite en la cantidad de apertura de casos, incidentes, solicitudes, requerimientos, consultas, soporte técnico, resolución de problemas.	x		Cumple de certificado de garantía técnica y soporte
270	Soporte 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante. El soporte debe incluir: - Apoyo en nuevas configuraciones. - Atención de incidentes (correo electrónico, teléfono, mesa de ayuda). - Instalación de nuevas actualizaciones (si aplica) - Un mantenimiento general en el año. - Atención de casos de carácter técnico en temas funcionales de las diferentes aplicaciones las cuales estén siendo protegidas en la presente solución.	x		Cumple de certificado de garantía técnica y soporte
271	Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al mismo, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).	x		Cumple de certificado de garantía técnica y soporte
272	El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá	x		Cumple de certificado de garantía técnica y soporte
273	El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket de servicio para los incidentes presentados	x		Cumple de certificado de garantía técnica y soporte
274	Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad	x		Cumple de certificado de garantía técnica y soporte

No.	Obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	ALCANCE GARANTÍA TÉCNICA			
275	GARANTÍA: El término de la garantía técnica o garantía legal de conformidad con los artículos No. 7, 8, 9 y 11 de la Ley 1480 de 2011, será de dos (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante	x		Cumple de certificado de garantía técnica y soporte
276	Se debe efectuar como mínimo dos (02) mantenimientos preventivos a la solución descrita en el presente anexo, por el término de la garantía	x		Cumple de certificado de garantía técnica y soporte
277	Estos mantenimientos deben incluir como mínimo las siguientes actividades: - Actualizaciones y Parches de Seguridad * Aplicación de actualizaciones y parches de seguridad críticos en el WAF. * Revisión periódica de las nuevas versiones del WAF y su impacto en la configuración actual. - Revisión y Solución de Errores * Monitoreo y resolución de errores o fallos en las reglas de seguridad. * Identificación y mitigación de falsos positivos y falsos negativos en la protección del WAF. - Copias de Seguridad y Recuperación * Programación y validación de copias de seguridad de configuraciones y reglas de seguridad. * Plan de recuperación en caso de incidentes o errores de configuración. - Monitoreo y Análisis de Logs * Revisión periódica de logs de actividad y eventos de seguridad. * Generación de reportes sobre ataques detectados y acciones de mitigación aplicadas. - Optimización de Recursos * Análisis del consumo de recursos en la nube y optimización de configuraciones. * Ajustes en las reglas de caching y mitigación de ataques para mejorar la disponibilidad y rendimiento del servicio. - Desactivación de Funcionalidades Inoperativas * Identificación y eliminación de reglas o configuraciones obsoletas o ineficaces. * Mantenimiento de una configuración optimizada basada en buenas prácticas. - Procedimientos de Hardening * Implementación de medidas de refuerzo de seguridad recomendadas por los principales proveedores de WAF en la nube. * Configuración avanzada de mitigación de amenazas (Rate Limiting, Bot Management, Geo-blocking, etc.). - Nuevas implementaciones. Las ventanas de mantenimiento deben ser programados en horarios no hábiles, previas coordinaciones con el Supervisor del contrato y de acuerdo con las necesidades del COGFM	x		Cumple de certificado de garantía técnica y soporte
278	En caso de presentarse fallas en la solución de seguridad descrita en el anexo, se deberán efectuar los acompañamientos todas las veces que se requiera. Estos deben incluir como mínimo: - Remplazo de la solución de seguridad por otra de iguales o superiores características. - Instalación y/o reparación de software. - Configuraciones, puesta en producción y funcionamiento	x		Cumple de certificado de garantía técnica y soporte
279	El servicio será brindado en sitio en la ciudad de Bogotá de acuerdo con los tiempos de respuesta establecidos	x		Cumple de certificado de garantía técnica y soporte
280	El tiempo máximo permitido para cambio o reparación de la solución de seguridad es de 20 días calendario una vez sea reportado el incidente, en caso que la falla genere afectación de servicio el contratista deberá suministrar, configurar y poner en funcionamiento temporalmente, una solución, de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para COGFM, con el fin de garantizar la continuidad en la prestación de los servicios	x		Cumple de certificado de garantía técnica y soporte
281	El contratista deberá suministrar, configurar y poner en perfecto funcionamiento la solución de seguridad, después de realizar el mantenimiento (cuando aplique), garantizando la continuidad de los servicios	x		Cumple de certificado de garantía técnica y soporte
282	En caso de que la solución de seguridad genere la reinstalación o reconfiguración de software, sistema operativo o firmware, estas labores deben ser realizadas por el contratista sin costo adicional para el COGFM	x		Cumple de certificado de garantía técnica y soporte

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
283	Todos los gastos que se ocasionen por concepto de transporte y otros gastos a fin de cumplir con los mantenimientos preventivos y correctivos correrán por cuenta del contratista	x		Cumple de certificado de garantía técnica y soporte
	FUNCIONAMIENTO Y CONTINUIDAD			
284	Garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados por la solución de seguridad descrita en este anexo, a partir de la fecha de activación del producto	x		Se realiza la activación del producto y no se presentan intermitencias
285	Se debe garantizar el funcionamiento de cada uno de los elementos de software del SISTEMA DE SEGURIDAD, mínimo durante el tiempo de la garantía técnica, reemplazando durante dicho periodo, cualquier elemento del software en falla o mal funcionamiento	x		Se mantiene en funcionamiento
	ACTUALIZACIONES			
286	Durante el tiempo de la garantía se debe brindar e instalar actualizaciones a la solución de seguridad descrita en el presente anexo, cada vez que se libere en el mercado una nueva versión de software, upgrade, o parche. Lo anterior previa solicitud y aprobación del supervisor del contrato y una vez haya sido probada en laboratorio, asegurando la continuidad del servicio y funcionamiento de los sistemas	x		La aplicación tiene actualización disponible durante el tiempo de vigencia de las licencias
287	Se debe realizar entrega al COGFM, de los medios magnéticos y/o manuales si existen cambios de versión	x		se entregan los manueles en medio magnético y se almacenan de en la carpeta c://waf de computador de administrador de la plataforma
	REPORTES E INFORMES TÉCNICOS			
288	Una vez realizados los acompañamientos (remotos o en sitio), se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar: - Actividades realizadas. - Actualizaciones aplicadas. - Procedimientos preventivos y/o correctivos aplicados. - Recomendaciones. - Pendientes	x		se realiza informe técnico de instalación que reposa en el computador del administrador por contener información de configuración de seguridad
	SEGURIDAD			
289	ACUERDO DE CONFIDENCIALIDAD: El Contratista y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista, lo cual será verificado por el supervisor del contrato	x		Se firman los acuerdos de confidencialidad por parte del contratista
290	Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares	x		El contratista acepta las políticas de seguridad informática
291	El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará	x		El contratista acepta las políticas de seguridad informática
	OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO			
292	El contrato debe ejecutarse a todo costo, el contratista se compromete a realizar la suscripción con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad	x		No se generan sobre costos en la implementación del proceso
293	El contratista deberá realizar transferencia de conocimiento y entrenamiento como mínimo de 20 horas, en el manejo y administración de la plataforma de protección de aplicaciones web. Adicionalmente suministrar el respectivo voucher para presentar examen de certificación como técnico especialista ante el fabricante de la solución	x		Se anexan los soportes de la transferencia de conocimientos

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE SI	CUMPLE NO	OBSERVACIONES
	de seguridad, para tres (03) funcionarios del CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM			
294	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia, en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se dispone de los recursos necesarios para la implementación del presente contrato
295	Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista deberá presentar el cronograma de actividades para la ejecución del objeto del contrato, para aprobación del supervisor del contrato	x		Se aprueba el cronograma ejecución del contrato
296	PERSONAL PARA LA EJECUCIÓN DEL CONTRATO - INGENIERO DE SOPORTE E IMPLEMENTADOR DE LA SOLUCIÓN DE SEGURIDAD: JUAN PABLO MACÍAS VARGAS. Ingeniero Telecomunicaciones	x		Se verifica la documentación y ne anexa planilla de pago de seguridad social
297	En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario. Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa	x		No se realizaron cambios en el personal
298	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto	x		No se realizaron cambios en el personal
299	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado	x		Se verifican las planilla de pagos de seguridad social y parafiscales y se adjunta copia
300	El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato	x		El personal realiza la implementación de la solución de acuerdo a lo solicitado en la ficha técnica
301	Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Se leen los pliegos, se crea el cronograma de ejecución de acuerdo a la ficha técnica
302	El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato	x		el contratista cumple con las normas de seguridad industrial
303	El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma			El contratista se hace cargo del personal que participa en la implementación del contrato
	Ponderables			
	LOTE 2			
1	El Contratista ofrece sin costo adicional: la actualización del fortiAnalyzer a la versión VM y que cuente con una capacidad mínima de procesamiento de +100gb por día de logs, sin que este ofrecimiento genere costo adicional para el COGFM	x		Se realiza la actualización a la versión VM con capacidad de +100G
2	El Contratista ofrece sin costo adicional: 25 horas de transferencia de conocimiento en administración y configuración del Proxy para (02) dos funcionarios del CGDJ6 con Voucher incluido, sin que este ofrecimiento genere costo adicional para el COGFM	x		Se realiza la entrega de los Voucher

No.	Obligaciones especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	CUMPLE		OBSERVACIONES
		SI	NO	
	LOTE 3			
3	El contratista ofrece sin costo adicional: transferencia de conocimiento de la solución de protección de datos ofertada con certificación de Voucher para cuatro (04) funcionarios del Comando General de las Fuerzas Militares – CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.	x		Se anexa el vaucher del ponderable
	LOTE 5			
4	El contratista ofrece sin costo adicional: Terminal para administración y gestión de la solución de seguridad que debe incluir como mínimo Intel® Core™ Ultra 7 265KF, Windows 11 Pro, NVIDIA® GeForce RTX™ 5080, 32 GB DDR5, SSD de 2 TB, Con periféricos incluidos y 02 dispositivos de visualización de 25" que permitan visualización y monitoreo de datos críticos, sin que este ofrecimiento genere costo adicional para la entidad	x		Se realiza la entrada al almacen de computador Workstation

4. Cumplimiento de Obligaciones al Sistema de Seguridad Social y Parafiscales

Que la Planilla Integrada de Liquidación de Aportes N° 91346758 con fecha de pago 21 de noviembre y 92119873, con fecha de pago 05 de diciembre de 2025, evidencian el cumplimiento de las obligaciones al Sistema de Seguridad Social Integral, la cual es anexada al presente informe.

Que mediante certificación de fecha 01 de diciembre de 2025, suscrita por la Señora Diana Maria Mendez Garnica , revisor fiscal con TP. No 193872-T, de la empresa HEIMCORE SAS ,, estipula encontrarse al día en el pago al Sistema de Seguridad Social en Pensiones y en Salud, riesgos profesionales, aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje (SENA) que mediante certificación de fecha 09 de diciembre de 2025, suscrita por la Señor Franklin Barrera castañeda , revisor fiscal con TP. No 172038-T, de la empresa YEAPDATA SAS ,, estipula encontrarse al día en el pago al Sistema de Seguridad Social en Pensiones y en Salud, riesgos profesionales, aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje (SENA) . Se anexa certificado del cumplimiento por parte del contratista.

NOTA: El certificado de aportes parafiscales lo puede firmar el representante legal cuando en cámara de comercio no reporta revisor fiscal, cuando el contratista tiene revisor fiscal este es el único competente para firmar las certificaciones de paz y salvo de seguridad social y parafiscal.

5. Aspectos Financieros

Valor Inicial del Contrato Incluido IVA:	$1.769.215.000
Que al contrato se le efectuó una adición el XX de XXX de 20XX por valor de:	$ 0
Valor Total del Contrato es de:	$1.769.215.000

Que se tramitaron las siguientes facturas con cargo al contrato supervisado:

No Factura	Fecha	Valor de la Factura
FV2	24-10-2025	$294.000.000
FV5	12-12-2025	$387.700.000
FV6	12-12-2025	$1.087.515.000
Valor Facturado		$1.769.215.000
Saldo por Facturar		$ 0
Valor de Reintegro		$ 0
Valor Total del Contrato		$1.769.215.000

6. Observaciones relevantes del supervisor: se realizo la entrega de la licencias contratadas de acuerdo al anexo técnico, verificando la consola y la vigencia de las mismas, así mismo lo informes técnicos por contener información secreta de configuración de seguridad se encuentran de manera digital en el computador del administrador de la plataforma.

7. Documentos anexos:

certificado de entrega de licencias
certificado capacitación
compromiso de confiabilidad
Cronograma de Actividades
Certificado SST
Certificado de para fiscales
Certificado de pago seguridad social.

Atentamente,

Mayor JOSE FRANCISCO LOMBANA CARDONA
Supervisor
Correo electrónico flombanac@gmail.com
No. de contacto 3165775377

Espacio para ser diligenciado en la Dirección Administrativa y Financiera

CONTROL DE APROBACIONES Y DE TIEMPOS PARA PUBLICAR				
CONTRATOS	FECHA DE RECEPCIÓN DEL INFORME	FECHA DE APROBACIÓN Y CARGUE DEL INFORME.	NOMBRE DE FUNCIONARIO REVISOR	FIRMA DEL FUNCIONARIO AVALANDO INFORME
	30 Dic/25	30 Dic/25	Profesional de Tesorería 30 Dic/25 10:45AM	

TEMARIO DE TRANSFERENCIA DE CONOCIMEINTOS – SUSCRIPCIÓN WAF

Duración total: 20 horas
Modalidad: Teórico
Fecha de Inicio: 20 de octubre 2025
Fecha de Finalización: 24 de octubre de 2025

MATERIAL DE ESTUDIO

Para cada uno de los estudiantes se entregó el siguiente material:

- Acceso a la plataforma F5 Learning Center
- Acceso a F5 Cloud Docs
- Guías de estudio y laboratorios: Balanceo de carga (Load Balancing), seguridad de aplicaciones (WAF), entrega de aplicaciones, nube, DNS, y tecnologías como BIG-IP
- Libreta de notas

Objetivo general:

Capacitar al equipo de CGFM para administrar y operar de forma autónoma el servicio WAF F5 Distributed Cloud Services (F5XC/WAAP), incluyendo el entendimiento de la arquitectura implementada, la gestión de Workspaces, la configuración y administración de Load Balancers, Origin Pools, App Firewall y certificados TLS, el uso de modos de operación (alerting/bloqueo), el análisis de eventos y métricas, y la integración de logs hacia CrowdStrike para soportar la operación continua y las pruebas de aceptación de la solución.

A continuación, se relaciona el detalle de cada una de las sesiones:

- **Sesión 1 (4h) – Fundamentos y arquitectura de la solución WAF F5XC**
    - Contexto del servicio WAAP y capacidades principales (protección L7, OWASP Top 10, controles básicos).
    - Arquitectura F5XC (modelo SaaS/edge) y flujo de tráfico implementado (DNS → F5XC → origen).
    - Componentes clave: WAAP, App Firewall, Load Balancer, Origin Pool y gestión centralizada.
    - Actividad práctica: recorrido guiado por consola y revisión del diagrama/flujo de la solución.

FECHA	12 DICIEMRBE 2025	CIUDAD	BOGOTÁ D.C

[illegible]	COMANDO GENERAL DE LAS FUERZAS MILITARES
[illegible]	JOSE FRANCISCO LOMBANA CARDONA
[illegible]	316 5775377
DIRECCIÓN	Carrera 54 N°26-25 Barrio Esmeralda Bogotá

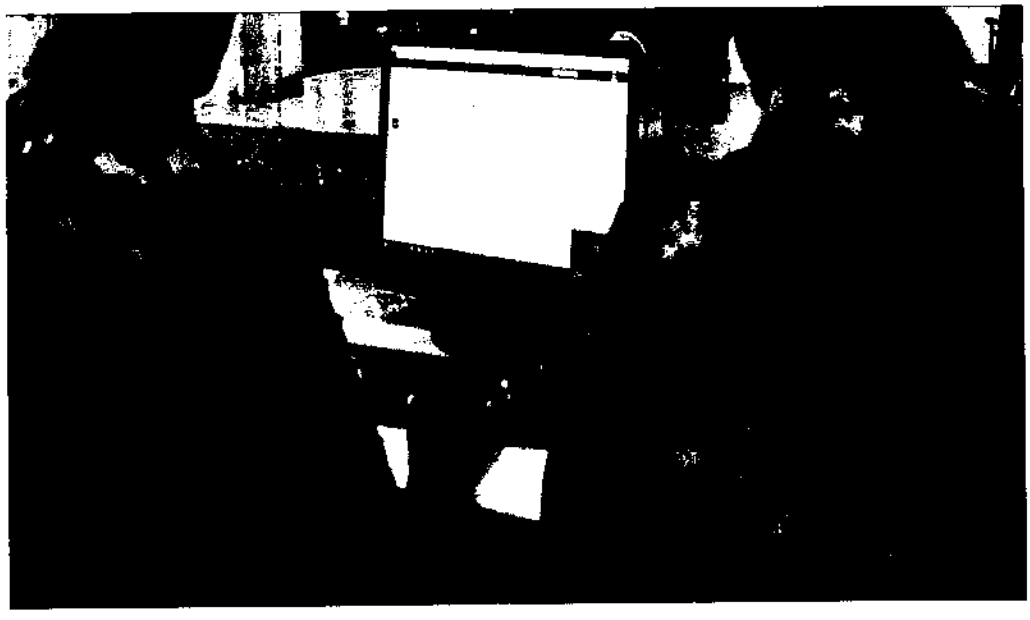
ACTA TRANSFERENCIA DE CONOCIMIENTOS

OBJETO DE CONTRATO

El contratista se obliga para con EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a prestar el servicio de mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 LOTE 2: LICENCIAS PROXY WEB ;LOTE 3: SUSCRIPCIÓN PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato.

TRANSFERENCIA DE CONOCIMIENTO LOTE 5 - SUSCRIPCIÓN WAF

Registro Fotográfico Transferencia de Conocimeinto



- **Sesión 9 (4h) – Respuesta a incidentes (end-to-end)**
    - Flujo estándar: triage → contención → erradicación → recuperación → lecciones aprendidas.
    - Gestión de casos: documentación, evidencias, responsables y criterios de cierre.
    - Escenarios: ransomware, credenciales comprometidas, ejecución sospechosa, lateral movement.
    - Taller: atención de un incidente simulado y elaboración de resumen ejecutivo.

- **Sesión 10 (4h) – Threat Hunting, protección de datos y reporting**
    - Metodología de caza: hipótesis, consultas/búsquedas, priorización de hallazgos.
    - Enfoque de protección de datos: monitoreo de eventos relevantes y recomendaciones (según capacidades licenciadas).
    - Dashboards y reportes: operativos y ejecutivos (cobertura, tendencias, tiempos de respuesta).
    - Cierre: checklist de operación, plan de mejora continua y próximos pasos (madurez SOC).

Cordialmente,

Enuar Emilio Rosales Salazar	COGFM	
Idier Loaiza Zabala	COGFM	
Fabian Joany Rodríguez Gómez	COGFM	
Wilson Oswaldo Vargas Córdoba	COGFM	
Jose Francisco Lombana Cardona	COGFM	
Carlos Giovani Díaz Rueda	UT 273COGFM H&Y 2025	

FECHA	12 DICIEMRBE 2025	CIUDAD	BOGOTÁ D.C

	COMANDO GENERAL DE LAS FUERZAS MILITARES
	JOSE FRANCISCO LOMBANA CARDONA
	316 5775377
	Carrera 54 N°26-25 Barrio Esmeralda Bogotá

ACTA TRANSFERENCIA DE CONOCIMIENTOS

OBJETO DE CONTRATO

El contratista se obliga para con EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a prestar el servicio de mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 LOTE 2: LICENCIAS PROXY WEB ;LOTE 3: SUSCRIPCIÓN PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato.

TRANSFERENCIA DE CONOCIMIENTO LOTE 3 - SUSCRIPCIÓN PROTECCIÓN DE DATOS

En cumplimiento de las **obligaciones contractuales** establecidas en el **Contrato 259COGFM DIADF 2025**, el presente apartado introduce la **transferencia de conocimiento** orientada a asegurar que el equipo designado cuente con los fundamentos técnicos y operativos para administrar Falcon CrowdStrike de forma autónoma y continua.

Registro Fotográfico Transferencia de Conocimeinto	
	

TEMARIO DE TRANSFERENCIA DE CONOCIMEINTOS – SUSCRIPCIÓN DE PROTECCIÓN DE DATOS - CROWDSTRIKE

Duración total: 40 horas
Modalidad: Teórico
Fecha de Inicio: 14 de octubre 2025
Fecha de Finalización: 27 de octubre de 2025

MATERIAL DE ESTUDIO

Para cada uno de los estudiantes se entregó el siguiente material:

- Acceso a la Página de Recursos de CrowdStrike
- Acceso a CrowdStrike University
- Guías impresas con información Plataforma Falcon, inteligencia de Amenazas, Caza de Amenazas y Respuesta a Incidentes
- Libreta de notas

Objetivo general:

La capacitación en Falcon CrowdStrike tiene como objetivo dejar al equipo en capacidad de operar y administrar la plataforma de forma autónoma, abarcando la configuración inicial de la consola, el despliegue y verificación del sensor en endpoints y servidores, la creación y ajuste de políticas de protección, la gestión de hosts y la visibilidad operacional, así como la detección, análisis y respuesta ante incidentes mediante capacidades EPP/Antimalware, EDR/XDR y respuesta en tiempo real, complementado con prácticas de caza de amenazas y lineamientos de protección de datos, orientados a fortalecer la postura de ciberseguridad y asegurar una operación continua y controlada.

A continuación, se relaciona el detalle de cada una de las sesiones:

- **Sesión 1 (4h) – Visión general y fundamentos**
    - Alcance del proyecto y objetivos operativos del SOC/área responsable.
    - Conceptos: EPP vs EDR vs XDR, telemetría, detección por comportamiento.
    - Arquitectura Falcon (Console, Sensor, módulos) y flujo de eventos.
    - Recorrido guiado por la consola: menús clave, vistas principales y buenas prácticas de navegación.

- **Sesión 2 (4h) – Configuración inicial y preparación operativa**
  - Creación/ajuste de **roles y permisos** (admin, analista, auditor) y segregación de funciones.
  - Parametrización base: alertas, notificaciones, retención/visibilidad (según licencia).
  - Reglas básicas de operación: naming convention, control de cambios y checklist de alistamiento.
  - Validación de prerequisitos y criterios de "plataforma lista para operar".

- **Sesión 3 (4h) – Despliegue del Sensor en Windows**
  - Métodos de instalación: manual, por herramientas de despliegue (GPO/SCCM/Intune u otras).
  - Paquetes, tokens/installer, verificación de instalación y comunicación con la nube.
  - Manejo de errores frecuentes (proxy, DNS, certificados, restricciones de red).
  - Laboratorio: instalación en un grupo piloto y validación de reporting en consola

---

- **Sesión 4 (4h) – Despliegue del Sensor en Linux y servidores**
  - Instalación en distribuciones Linux (paquetes, servicios, permisos) y consideraciones en servidores.
  - Actualización/versionamiento del sensor y política de mantenimiento.
  - Validación de telemetría, salud del host y diagnóstico de conectividad.
  - Laboratorio: despliegue en servidor Linux y checklist de "host protegido".

- **Sesión 5 (4h) – Gestión de Hosts e inventario**
  - Inventario: estados del sensor, cobertura, etiquetas y clasificación por criticidad.
  - Creación de **grupos** por área de negocio/entorno (producción, pruebas, usuarios).

- Acciones remotas básicas sobre hosts (aislamiento, contención, recolección de info según permisos).
- Rutina diaria: revisión de salud, endpoints sin sensor, endpoints inactivos y recomendaciones.

- **Sesión 6 (4h) – Políticas de protección y afinamiento**
  - Estructura de políticas: prevención, comportamiento, control de ejecución (según módulos).
  - Asignación por grupos y estrategia "baseline + excepciones controladas".
  - Gestión de exclusiones: criterios, trazabilidad, vigencia y revisión periódica.
  - Taller: creación de política para endpoints y otra para servidores + plan de tuning.

- **Sesión 7 (4h) – Antivirus/Antimalware y prevención**
  - Configuración de prevención y respuesta ante malware (bloqueo, cuarentena, remediación).
  - Gestión de falsos positivos: validación, evidencia, ajuste de exclusiones con control.
  - Pruebas controladas (no disruptivas) para validar detección y respuesta.
  - Recomendaciones para mantener equilibrio entre seguridad y operación.

- **Sesión 8 (4h) – Detección y respuesta EDR/XDR**
  - Interpretación de detecciones: severidad, táctica/técnica, contexto del endpoint.
  - Correlación y análisis: línea de tiempo, procesos, indicadores y evidencia.
  - Acciones de contención: aislamiento del host, bloqueo, medidas inmediatas.
  - Introducción práctica a RTR (respuesta en tiempo real): uso responsable y registros.

- **Sesión 2 (4h) – Consola SaaS y Workspaces (operación y gobierno)**
    - Acceso a la consola, estructura de la organización y mejores prácticas operativas.
    - Workspaces: propósito, segmentación y enfoque por funciones (WAAP y Multi-Cloud Networking).
    - Gestión de usuarios/roles (RBAC) y lineamientos de control de cambios.
    - Actividad práctica: validación de permisos, navegación por Workspaces y checklist de operación inicial.

- **Sesión 3 (4h) – Publicación y continuidad: Load Balancer, Origin Pools y dominios protegidos**
    - Configuración/validación de Load Balancers como punto de entrada (aplicación de políticas WAAP).
    - Origin Pools: definición de orígenes, health checks y consideraciones de continuidad del servicio.
    - Relación dominio–LB–origen y validación de conectividad end-to-end.
    - Actividad práctica: revisión de configuración de LBs y pools existentes, y verificación de salud/flujo.

- **Sesión 4 (4h) – App Firewall (WAF): políticas, OWASP y afinamiento (tuning)**
    - App Firewall: propósito, lógica de inspección y políticas basadas en comportamiento/firmas.
    - Modos de operación: monitoreo/alerting vs bloqueo/enforcement (puesta en producción controlada).
    - Ajuste de políticas: manejo de excepciones seguras, reducción de falsos positivos y trazabilidad.
    - Actividad práctica: análisis de eventos de ejemplo, identificación de falsos positivos y propuesta de tuning.

- **SESIÓN 5 (4h) – Certificados TLS, observabilidad e integración con CrowdStrike (cierre operativo)**
    - Certificados TLS: terminación HTTPS en el LB, inspección en claro y re-cifrado hacia backend (buenas prácticas).
    - Métricas, tableros y reportes operativos (qué revisar y con qué frecuencia).
    - Integración de eventos hacia CrowdStrike: concepto y validación del envío (Global Log Receiver "HTTPS Receiver").
    - Actividad práctica: verificación de registros/eventos, revisión de pruebas de aceptación y checklist de operación continua.

Cordialmente,

Nombre	Entidad	Firma
Enuar Emilio Rosales Salazar	COGFM	
Idier Loaiza Zabala	COGFM	
Wilson Oswaldo Vargas Córdoba	COGFM	
Jose Francisco Lombana Cardona	COGFM	
Carlos Giovani Díaz Rueda	UT 273COGFM H&Y 2025	

Carlos Giovani Diaz Rueda

De: Frank Gualdron <f.gualdron@f5.com>
Enviado el: miércoles, 12 de diciembre de 2025 11:25 a. m.
Para: Carlos Giovani Diaz Rueda
CC: Andres Rodrigo Rodriguez Castañeda
Asunto: Re: [External] Voucher para tres (03) funcionarios - F5

Thank you for reaching out. Please find below the exam voucher codes for your account. Kindly ensure they are used to schedule and complete exams on or before the listed expiration date.

Voucher Code	Voucher Expiration Date	Voucher Status
F5-9K3D-V7Q2-LX8P	09/30/2026	Available
F5-H4T6-2WQN-8JRC	09/30/2026	Available
F5-Z1M8-R5Y3-6PVA	09/30/2026	Available

Please follow these steps when you're ready to take your F5 Certification Exam:

1. Sign in to F5 University
2. If this is your first time taking an F5 certification exam, locate your F5 University ID in your profile and keep it handy – you will need it when creating your exam taker account with Pearson VUE.
3. From the F5 University homepage, select Certification (or Get Certified, depending on what you see).
4. Select Schedule your certification exam. This will redirect you to the Pearson VUE / F5 site, where you can create your exam taker account and register for your exam.
5. If you run into scheduling issues online, you can contact Pearson VUE to schedule your exam by phone.
6. When creating your exam taker account profile, make sure to include your F5 University ID.

COMPROMISO CONFIDENCIALIDAD

SERA DILIGENCIADO AL MOMENTO DE SUSCRIPCIÓN DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mí propio nombre y de los funcionarios o asesores que se vinculen a la misma para efectos de ejecución del presente contrato, asume el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que el **MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA** adelantó el proceso de selección del Contrato de No. 259 , cuyo objeto es PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO.

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares del Ministerio a los cuales tenga acceso.

CUARTA: Que acepto y permito al Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, utilizar de manera responsable y de acuerdo con la política de protección de datos personales, la información que he proporcionado, para lo cual garantizó que son exactos, por lo que, en caso de ser modificados, comunicaré al Ministerio, para que sean rectificados y/o cancelados según proceda.

QUINTA: **Que, por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:**

CLÁUSULA PRIMERA. COMPROMISO ASUMIDO POR EL CONTRATISTA: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

EL CONTRATISTA se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.

b) No permitir que terceros obtengan información relacionada con el literal anterior.

c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

e) No dar, ofrecer dadivas, regalos, beneficios, comisiones, promesa remuneratoria, directa o indirectamente; tanto en el ministerio o fuera de él, a cambio de obtener beneficios ilegales en la ejecución de sus obligaciones contractuales.

f) Fomentar el reporte de conductos, hechos que puedan llegar a configurasen en prácticas de soborno, corrupción, con fundamento en la buena fe o en una sospecha razonable.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: EL CONTRATISTA asume a través de la suscripción del presente compromiso, las consecuencias que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente EL CONTRATISTA que toda la información que se produzca en la ejecución del contrato será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá, D.C. a los (09) días del mes de octubre del dos mil veinticinco (2025).

EL CONTRATISTA

Nombre: RONALD ALEXANDER CASTAÑEDA
C.C. No. 80.195.893

COMPROMISO CONFIDENCIALIDAD

SERA DILIGENCIADO AL MOMENTO DE SUSCRIPCIÓN DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mi propio nombre y de los funcionarios o asesores que se vinculen a la misma para efectos de ejecución del presente contrato, asume el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que el **MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA** adelantó el proceso de selección del Contrato de No. 259 , cuyo objeto es PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO.

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares del Ministerio a los cuales tenga acceso.

CUARTA: Que acepto y permito al Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, utilizar de manera responsable y de acuerdo con la política de protección de datos personales, la información que he proporcionado, para lo cual garantizó que son exactos, por lo que, en caso de ser modificados, comunicaré al Ministerio, para que sean rectificados y/o cancelados según proceda.

QUINTA: **Que, por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:**

CLÁUSULA PRIMERA. COMPROMISO ASUMIDO POR EL CONTRATISTA: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

EL CONTRATISTA se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.

b) No permitir que terceros obtengan información relacionada con el literal anterior.

c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

e) No dar, ofrecer dadivas, regalos, beneficios, comisiones, promesa remuneratoria, directa o indirectamente; tanto en el ministerio o fuera de él, a cambio de obtener beneficios ilegales en la ejecución de sus obligaciones contractuales.

f) Fomentar el reporte de conductos, hechos que puedan llegar a configurasen en prácticas de soborno, corrupción, con fundamento en la buena fe o en una sospecha razonable.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: EL CONTRATISTA asume a través de la suscripción del presente compromiso, las consecuencias que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente EL CONTRATISTA que toda la información que se produzca en la ejecución del contrato será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá, D.C. a los (09) días del mes de octubre del dos mil veinticinco (2025).

EL CONTRATISTA

Nombre: JUAN PABLO MACIAS VARGAS
C.C. No. 1.032.363.649

COMPROMISO CONFIDENCIALIDAD

SERA DILIGENCIADO AL MOMENTO DE SUSCRIPCIÓN DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mí propio nombre y de los funcionarios o asesores que se vinculen a la misma para efectos de ejecución del presente contrato, asume el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que el **MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA** adelantó el proceso de selección del Contrato de No. 259 , cuyo objeto es PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO.

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares del Ministerio a los cuales tenga acceso.

CUARTA: Que acepto y permito al Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, utilizar de manera responsable y de acuerdo con la política de protección de datos personales, la información que he proporcionado, para lo cual garantizó que son exactos, por lo que, en caso de ser modificados, comunicaré al Ministerio, para que sean rectificados y/o cancelados según proceda.

QUINTA: **Que, por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:**

CLÁUSULA PRIMERA. COMPROMISO ASUMIDO POR EL CONTRATISTA: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

EL CONTRATISTA se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.

b) No permitir que terceros obtengan información relacionada con el literal anterior.

c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

e) No dar, ofrecer dadivas, regalos, beneficios, comisiones, promesa remuneratoria, directa o indirectamente; tanto en el ministerio o fuera de él, a cambio de obtener beneficios ilegales en la ejecución de sus obligaciones contractuales.

f) Fomentar el reporte de conductos, hechos que puedan llegar a configurasen en prácticas de soborno, corrupción, con fundamento en la buena fe o en una sospecha razonable.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: EL CONTRATISTA asume a través de la suscripción del presente compromiso, las consecuencias que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente EL CONTRATISTA que toda la información que se produzca en la ejecución del contrato será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá, D.C. a los (09) días del mes de octubre del dos mil veinticinco (2025).

EL CONTRATISTA

Nombre: EDGAR ALFONSO GODOY LOPEZ
C.C. No. 79.906.707

Yeapdata

Heimcore

Bogotá, 08 de octubre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: Entrega de formatos de seguridad del personal asignado al contrato No. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del Contrato No. 259COGFM DIADF 2025, la Unión Temporal UT273COGFM H&Y 2025, en calidad de Contratista, manifiesta la entrega de los formatos del personal que realizará la ejecución del contrato cuyo objeto es prestar el servicio de mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 LOTE 2: LICENCIAS PROXY WEB ;LOTE 3: SUSCRIPCIÓN PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato.

En atención al requerimiento de entrega de los formatos de seguridad, nos permitimos relacionar el personal que entrega la documentación requerida:

No.	NOMBRES Y APELLIDOS	IDENTIFICACIÓN
1	EDGAR ALFONSO GODOY LOPEZ	79.906.707
2	JUAN PABLO MACIAS VARGAS	1.032.363.649
3	VICTOR MANUEL MENDOZA ANAYA	80.113.599
4	RONALD ALEXANDER CASTAÑEDA	80.195.893

De esta manera, la Unión Temporal UT273COGFM H&Y 2025 ratifica el cumplimiento de los compromisos adquiridos y reitera su disposición para atender cualquier requerimiento adicional que contribuya al correcto desarrollo del contrato

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Heimcore

CERTIFICACIÓN DE CUMPLIMIENTO ARTICULO 50 LEY 798 DE 2002 Y LEY 828 DE 2003

PERSONA JURIDICA

Yo, **DIANA MARIA MENDEZ GARNICA** identificado con cédula de ciudadanía No. **39.804.649**, de Cajica y con Tarjeta Profesional No.193872-T de la Junta Central de Contadores de Colombia, en mi condición de **REVISOR FISCAL** de **HEIMCORE SAS**, identificada con Nit. **900.425.697-2** debidamente inscrito ante la Cámara de Comercio de Bogotá, luego de examinar de acuerdo con las normas de auditoria generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico el pago de los aportes de seguridad social (pensión, salud y riesgos laborales) y de los aportes parafiscales (Instituto Colombiano de Bienestar familiar ICBF, Servicio Nacional de Aprendizaje SENA y Caja de Compensación Familiar), Obligaciones laborales, salaries y prestaciones sociales, cuando a ello hubiere lugar pagados por la compañía durante los últimos seis (6) meses legalmente exigibles a la fecha de la emisión de esa certificación, dichos pagos corresponden a los montos contabilizados y cancelados por la compañía durante dichos 6 meses. Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

Nota 1: Para certificar el pago de los aportes correspondientes a los Sistemas de Seguridad Social y en el caso del pago correspondiente a los aportes parafiscales, se deberán tener en cuenta los plazos previstos de Decreto 1670 de 2007.

Se expide en Bogotá D.C, al primero de diciembre de 2025.

DIANA MARIA MENDEZ GARNICA
REVISOR FISCAL
C.C. 39.804.649 de Cajica
T.P. 193872-T

GEDESPROS.A.S
NIT: 900695249 - 3

BOKS INTERNATIONAL

EL SUSCRITO REVISOR FISCAL DE
YEAPDATA SAS
NIT 900.311.748-1

CERT-056 09-12-2025 - YEAP

CERTIFICA QUE:

YEAPDATA SAS identificada con **NIT No. 900.311.748-1** (En adelante la Compañía), efectuó los aportes parafiscales (SENA, ICBF y Cajas de Compensación Familiar), seguridad social (Pensión y ARL) correspondiente al mes de **noviembre** del Dos Mil Veinticinco (2025), y de salud del mes de **diciembre** del Dos Mil Veinticinco (2025), según la planillas **No. 92124350** y **92119873** liquidada y pagada a través del operador de información "Aportes en Línea" las cuales fueron canceladas el Cinco (05) de diciembre del Dos Mil Veinticinco (2025).

La Compañía ha dado cumplimiento a los dispuesto en la **Ley 100 De 1993, Ley 789 De 2002 (Art 50), Ley 797 De 2003; Decreto 1703 De 2002, Decreto 2170 De 2002** y demás normas vigentes relacionadas con el pago de obligaciones de Sistema de Seguridad Social Integral y Aportes Parafiscales.

A la fecha de expedición de la presente, la Compañía se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral y lo que corresponde a Aportes Parafiscales de los Once (11) meses anteriores a esta certificación

Se expide la presente certificación en la ciudad de Bogotá a los Nueve (09) días de diciembre del año Dos Mil Veinticinco (2025), a solicitud de la administración de la Compañía.

Cordialmente,

FRANKLIN E. BARRERA CASTAÑEDA
Revisor Fiscal
Tarjeta Profesional No. 172038-T
Designado por **GEDESPRO S.A.S.**
Tarjeta de Registro No. 1787

AK 45 #122-56 / Ofi. 709
Edificio Argenta - Bogotá D.C

(601) 9260160 - 301 4764654

administrativoRRHH@gedespro.com.co

www.gedespro.com.co

THE WINNER

República de Colombia
Ministerio de Comercio Industria y Turismo

JUNTA CENTRAL DE CONTADORES
TARJETA PROFESIONAL
DE CONTADOR PUBLICO

193872-T



DIANA MARCELA
MENDEZ GARNICA
C.C. 39804849
RESOLUCION INSCRIPCION 1337 FECHA 09/09/2014
UNIVERSIDAD ECCI

DIRECTOR GENERAL

JULIO CESAR ACUÑA GONZALEZ 203099

195208

Esta tarjeta es el unico documento que lo acredita como CONTADOR PUBLICO de acuerdo con lo establecido en la ley 43 de 1990.
Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: 644 44 50 o devolverla a la UAE - Junta Central de Contadores a la calle 96 No. 9A - 21 Bogota D.C.

www.ideqs.com

compensar | miplanilla.com

REPORTE RESUMEN DE PAGO

Información básica de la planilla

Empresa:	HEIMCORE SAS	**NIT:**	900425697
Tipo Planilla:	E	**Periodo liquidación Pensiones:**	octubre 2025
Sucursal o Dependencia:	PRINCIPAL	**Periodo liquidación Salud:**	noviembre 2025
Número de Radicación:	91346758	**Total a pagar:**	$281,618,700
Fecha de vencimiento:	26/11/2025	**Total de empleados:**	200
Fecha de Pago:	21/11/2025	**Número de Administradoras:**	25

Detalles del pago

Razón social recaudo:	Compensar OI	**Nit recaudo:**	9998600669427
Descripción:	MiPlanilla.com Pago Proteccion Social	**Medio de Pago:**	Pago Electronico por PSE
Banco:	BANCO DE BOGOTA	**Número Autorización:**	1945289551
Estado de la transacción:	Transacción aprobada		

Código	NIT	Administradoras	Num. Afiliados	*Número de Incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
14-11	890903790	ARL SURA	200		$0	$9,801,700
230201	800229739	Proteccion (ING + Proteccion)	50		$0	$40,225,400
230301	800224808	Porvenir	86		$0	$52,828,600
230901	800253055	Skandia Fondo de Pensiones Obligatorias	5		$0	$9,802,100
231001	800227940	Colfondos	27		$0	$25,865,600
25-14	900336004	Administradora Colombiana de Pensiones -	28		$0	$29,453,200
CCF04	890900841	Comfama Caja de Compensacion Fliar	2		$0	$582,200
CCF06	890102002	Combarranquilla Caja de Compensacion Fliar	3		$0	$536,000
CCF13	891190047	Comfaca Caja de Compensacion Fliar	1		$0	$64,000
CCF24	860066942	Compensar Caja de Compensacion Fliar	184		$0	$36,222,900
CCF39	890200106	Cajasan Caja de Compensacion Fliar	1		$0	$64,000
CCF44	891480000	Comfamiliar Risaralda Caja de Compensacion Fliar	2		$0	$134,400
CCF48	800211025	Comfatolima Caja de Compensacion Fliar	1		$0	$64,000
CCF57	890303208	Comfamiliar Andi Comfandi Caja de	2		$0	$224,000
EPS001	830113831	ALIANSALUD EPS S.A.	10		$0	$7,864,700
EPS002	800130907	Salud Total EPS	27		$0	$8,688,100
EPS005	800251440	Sanitas EPS	67		$0	$25,231,900

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE							
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS		Carrera 198 # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A - Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ, D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS001	ALIANSALUD EPS S.A.	830113831-0	2.339.000	0		0		0	0	0	0	2.339.000	5
EPS002	Salud Total EPS	800130907-4	2.122.900	0		0		0	0	0	0	2.122.900	22
EPS005	Sanitas EPS	800251440-6	12.574.800	0		0		0	0	0	0	12.574.800	54
EPS008	Compensar EPS	860066942-7	5.363.200	0		0		0	0	0	0	5.363.200	39
EPS010	EPS Sura	800088702-2	2.302.900	0		0		0	0	0	0	2.302.900	17
EPS017	Famisanar EPS	830003564-7	4.764.500	0		0		0	0	0	0	4.764.500	34
EPS037	Nueva EPS	900156264-2	791.200	0		0		0	0	0	0	791.200	9
EPSC25	Capresoca EPS	891856000-7	136.500	0		0		0	0	0	0	136.500	1
EPSC34	Recaudo SGP Capital Salud	900298372-9	27.700	0		0		0	0	0	0	27.700	1
MIN001	Fondo Sol y Gar Min Salud	901037916-1	292.100	0		0		0	0	0	0	292.100	3

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230201	Proteccion (ING + Proteccion)	800229739-0	16.226.500	0	0	99.000	99.000	0	0		16.424.500	36
230301	Porvenir	800224808-8	40.910.400	0	0	463.800	463.800	0	0		41.838.000	80
230901	Skandia Pensiones Obligatorias	800253055-2	6.958.700	0	0	121.500	121.500	0	0		7.201.700	8
231001	Colfondos	800227940-6	13.601.600	0	0	283.100	283.100	0	0		14.167.800	20
25-14	Colpensiones	800336004-7	27.126.600	0	0	342.900	342.900	0	0		27.812.400	41

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatoria	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-7	Seguros Bolivar S.A.	860002503-2	15.428.900				15.428.900	0	0	15.428.900			154.289	15.428.900	185

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF14	Comfacauca	891500182-0	253.100	0	0	253.100	2
CCF22	Colsubsidio	860007336-1	25.913.600	0	0	25.913.600	179
CCF34	Cotrem	892000146-3	412.500	0	0	412.500	3
CCF69	Comfacasanare	844003392-8	136.500	0	0	136.500	1

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE							
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS		Carrera 196 # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Colegiado	Aportante	Extranjero	Colom. exterior	Exonerado	IGE	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	COTIZACIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliada	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Días de Ausen.	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC	1014256751	BETANCOURT BARRERA JESICA ALEJANDRA	1	D			S																	230301	10.500.000	1.680.000	0	0	52.500	52.500	EPS005	10.500.000	420.000	14-7	10.500.000	3	255.800	CCF22	10.500.000	420.000	10.590.000	0	0	0	0
2	CC	80133620	AGUILAR GARCIA ALEX CRISTIAN	1	D			S								X									25-14	3.815.257	610.500	0	0	0	0	EPS005	3.815.257	152.700	14-7	3.815.257	3	93.000	CCF22	3.815.257	152.700	3.815.257	0	0	0	0
3	CC	79627591	AREVALO BUITRAGO ALEXANDER	1	D			N																	25-14	12.953.850	2.072.700	0	0	64.800	64.800	EPS001	12.953.850	1.619.300	14-7	12.953.850	3	315.800	CCF22	12.953.850	518.200	12.953.850	259.100	388.700	0	0
4	CC	52274897	VASQUEZ ROBAYO ALEXANDRA	1	D			S																	25-14	3.500.000	560.000	0	0	0	0	EPS005	3.500.000	140.000	14-7	3.500.000	3	85.300	CCF22	4.146.867	165.900	4.146.867	0	0	0	0
5	CC	52337501	GUTIERREZ DUQUE ANA CRISTINA	1	D			S								X									25-14	3.535.333	565.700	0	0	0	0	EPS002	3.535.333	141.500	14-7	3.535.333	3	86.200	CCF22	3.535.333	141.500	3.535.333	0	0	0	0
6	CC	52337501	GUTIERREZ DUQUE ANA CRISTINA	1	D			S									X								25-14	516.130	82.600	0	0	0	0	EPS002	516.130	20.700	14-7	516.130	3	0	CCF22	516.130	20.700	516.130	0	0	0	0
7	CC	52843373	QUINTERO CETINA ANA LUISA	1	D			S																	231001	7.000.000	1.120.000	0	0	35.000	35.000	EPS005	7.000.000	280.000	14-7	7.000.000	3	170.600	CCF22	7.000.000	280.000	7.000.000	0	0	0	0
8	CC	1010005905	CAMARGO PORRAS ANA SOFIA	1	D			S	X							X									230301	2.159.091	345.500	0	0	0	0	EPS005	2.159.091	86.400	14-7	2.159.091	3	52.600	CCF22	5.262.336	210.500	5.262.336	0	0	0	0
9	CC	1023976244	MARIN ACELDAS ANDRES ALEJANDRO	1	D			S	X							X									230301	454.667	72.800	0	0	0	0	EPS002	454.667	18.200	14-7	454.667	3	11.100	CCF22	1.370.626	54.800	1.370.626	0	0	0	0
10	CC	1018600611	CORREDOR TOBON ANDRES FELIPE	1	D			S								X									230301	2.668.666	427.000	0	0	0	0	EPS017	2.668.666	106.800	14-7	2.668.666	3	65.100	CCF22	2.668.666	106.800	2.668.666	0	0	0	0
11	CC	1000954518	MALDONADO BOLAÑOS ANDRES FELIPE	1	D			S								X									230201	2.668.666	427.000	0	0	0	0	EPS017	2.668.666	106.800	14-7	2.668.666	3	65.100	CCF22	2.668.666	106.800	2.668.666	0	0	0	0
12	CC	1018473110	MESSE AYALA ANDRES FELIPE	1	D			S																	230201	1.933.334	309.400	0	0	0	0	EPS008	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
13	CC	1018473110	MESSE AYALA ANDRES FELIPE	1	D			S										X							230201	72.166	11.600	0	0	0	0	EPS008	72.166	2.900	14-7	72.166	3	0	CCF22	72.166	2.900	72.166	0	0	0	0
14	CC	1098619398	RINCON ORTIZ ANDRES MAURICIO	1	D			S																	230301	7.000.000	1.120.000	0	0	35.000	35.000	EPS010	7.000.000	280.000	14-7	7.000.000	3	170.600	CCF22	7.000.000	280.000	7.000.000	0	0	0	0
15	CC	1106890585	TAPIAS PORTELA ANDRES MAURICIO	1	D			S								X									230301	4.437.334	710.000	0	0	0	0	EPS008	4.437.334	177.500	14-7	4.437.334	3	108.100	CCF22	4.437.334	177.500	4.437.334	0	0	0	0
16	CC	1015415552	ARAQUE MEJIA ANDRES FELIPE	1	D			S								X									230901	11.068.666	1.771.000	0	0	55.400	55.400	EPS008	11.068.666	442.800	14-7	11.068.666	3	289.700	CCF22	11.068.666	442.800	11.068.666	0	0	0	0
17	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	D			S								X									230301	737.332	118.000	0	0	0	0	EPS008	737.332	29.500	14-7	737.332	3	18.000	CCF22	737.332	29.500	737.332	0	0	0	0
18	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	D			S										X							230301	1.395.464	223.300	0	0	0	0	EPS008	1.395.464	55.900	14-7	1.395.464	3	0	CCF22	1.395.464	55.900	1.395.464	0	0	0	0
19	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	D			S													L				230301	66.667	10.700	0	0	0	0	EPS008	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
20	CC	53040273	GIL VARGAS ANGELA MARCELA	1	D			S																	231001	11.000.000	1.760.000	0	0	55.000	55.000	EPS001	11.000.000	440.000	14-7	11.000.000	3	268.000	CCF22	11.000.000	440.000	11.000.000	0	0	0	0
21	CC	1000364789	LOPEZ QUINTERO ANTONY FERNEY	1	D			S								X									230201	1.729.718	276.800	0	0	0	0	EPS005	1.729.718	69.200	14-7	1.729.718	3	42.200	CCF22	1.729.718	69.200	1.729.718	0	0	0	0
22	CC	34555978	TERAN ESTUPIÑAN BEATRIZ EUGENIA	1	D			S																	25-14	3.600.000	576.000	0	0	0	0	EPS010	3.600.000	144.000	14-7	3.600.000	3	87.700	CCF22	3.600.000	144.000	3.600.000	0	0	0	0
23	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	D			S								X									230201	1.637.842	262.100	0	0	0	0	EPS008	1.637.842	65.500	14-7	1.637.842	3	39.900	CCF22	1.637.842	65.600	1.637.842	0	0	0	0
24	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	D			S										X							230201	65.999	10.600	0	0	0	0	EPS008	65.999	2.700	14-7	65.999	3	0	CCF22	65.999	2.700	65.999	0	0	0	0
25	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	D			S													L				230201	53.333	8.600	0	0	0	0	EPS008	53.333	2.200	14-7	53.333	3	0	CCF22	53.333	2.200	53.333	0	0	0	0
26	CC	1110172102	PEDRAZA MENDOZA BENJAMIN	1	D			S								X									230301	1.741.393	278.700	0	0	0	0	EPS017	1.741.393	69.700	14-7	1.741.393	3	42.500	CCF22	1.741.393	69.700	1.741.393	0	0	0	0
27	CC	1000227194	CARDOZO RUBIANO BRAYAN LEONARDO	1	D			S	X							X									231001	811.150	129.800	0	0	0	0	EPS008	811.150	32.500	14-7	811.150	3	19.800	CCF22	1.135.392	45.500	1.135.392	0	0	0	0
28	CC	80180405	MARTINEZ CRUZ CARLOS ANDRES	1	D			S								X									230301	9.214.080	1.474.300	0	0	46.100	46.100	EPS005	9.214.080	368.600	14-7	9.214.080	3	224.500	CCF22	8.000.000	320.000	8.000.000	0	0	0	0
29	CC	1118546521	VEGA CARDENAS CARLOS ANDRES	1	D			S								X									230301	3.412.499	546.000	0	0	0	0	EPSC25	3.412.499	136.500	14-7	3.412.499	3	83.200	CCF69	3.412.499	136.500	3.412.499	0	0	0	0
30	CC	1012448626	MORENO CRUZ CESAR SANTIAGO	1	D			S																	230201	2.000.000	320.000	0	0	0	0	EPS005	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
31	CC	1030652618	MACIAS BLANCO CHRISTOPHER	1	D			S								X									231001	4.653.408	744.500	0	0	0	0	EPS002	4.653.408	186.200	14-7	4.653.408	3	113.400	CCF22	4.653.408	186.200	4.653.408	0	0	0	0
32	CC	1027340471	BELEÑO JARAMILLO CLAUDIA MIREYA	1	D			S								X									230201	2.234.181	357.500	0	0	0	0	EPS002	2.234.181	89.400	14-7	2.234.181	3	54.500	CCF22	2.234.181	89.400	2.234.181	0	0	0	0
33	CC	39673887	LONDOÑO GIL CLAUDIA YANET	1	D			S																	231001	1.500.000	240.000	0	0	0	0	EPS002	1.500.000	60.000	14-7	1.500.000	3	36.600	CCF22	1.500.000	60.000	1.500.000	0	0	0	0
34	CC	1013644752	DIAZ ROJAS CRISTIAN CAMILO	1	D			S								X									230301	2.391.877	382.800	0	0	0	0	EPS017	2.391.877	95.700	14-7	2.391.877	3	58.300	CCF22	2.391.877	95.700	2.391.877	0	0	0	0
35	CC	1015455880	GALINDO CASTRO CRISTIAN CAMILO	1	D			S								X									230201	2.585.227	413.700	0	0	0	0	EPS017	2.585.227	103.500	14-7	2.585.227	3	63.000	CCF22	2.585.227	103.500	2.585.227	0	0	0	0
36	CC	1017401928	GUERRERO REYES CRISTIAN CAMILO	1	D			S								X									230301	2.887.998	462.100	0	0	0	0	EPS008	2.887.998	115.600	14-7	2.887.998	3	70.400	CCF22	2.887.998	115.600	2.887.998	0	0	0	0
37	CC	1015064582	ROA GUEVARA CRISTIAN LEONARDO	1	D			S								X									231001	7.307.301	1.169.200	0	0	36.600	36.600	EPS008	7.307.301	292.300	14-7	7.307.301	3	178.100	CCF22	7.307.301	292.300	7.307.301	0	0	0	0
38	CC	1000364348	CELIS MARTINEZ DANIEL ALEJANDRO	1	D			S																	25-14	7.500.000	1.200.000	0	0	37.500	37.500	EPS005	7.500.000	300.000	14-7	7.500.000	3	182.700	CCF22	7.500.000	300.000	7.500.000	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
N	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD
					EMPLEADOS / UPC
PERIODO SALUD	PERIODO PENSIONES				185 / 0
2025-12	2025-11	E	05/12/2025	92119873	TOTAL A PAGAR
					$182.898.300

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Cotiza en el exterior	Exonerado	IRP	PRT	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	VTE	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario o Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cod. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
79	CC	1022376015	URIZA CAMARGO FRANCISCO JAVIER	1	0			S												X					231001	200.279	32.100	0	0	0	0	EPS010	200.279	8.100	14-7	200.279	3	0	CCF22	259.483	10.400	259.483	0	0	0	0
80	CC	1030640824	POBLADOR NAVAS FREED ALEXANDER	1	0			S	X							X									230301	578.545	92.600	0	0	0	0	EPS010	578.545	23.200	14-7	578.545	3	14.100	CCF22	1.974.641	79.000	1.974.641	0	0	0	0
81	CC	1115743751	CARVAJAL MANCHEGO GERMAN ALEXANDER	1	0			S								X									230301	2.006.666	321.100	0	0	0	0	EPS002	2.006.666	80.300	14-7	2.006.666	3	48.900	CCF22	2.006.666	80.300	2.006.666	0	0	0	0
82	CC	1115743751	CARVAJAL MANCHEGO GERMAN ALEXANDER	1	0			S										X							230301	71.345	11.500	0	0	0	0	EPS002	71.345	2.900	14-7	71.345	3	0	CCF22	71.345	2.900	71.345	0	0	0	0
83	CC	1032415426	SOSA MORENO GERSON MARTIN	1	0			S																	230301	9.000.000	1.440.000	0	0	45.000	45.000	EPS005	9.000.000	360.000	14-7	9.000.000	3	219.300	CCF22	9.000.000	360.000	9.000.000	0	0	0	0
84	CC	52714059	RAMAMON LOPEZ GIOVANNA CRISTINA	1	0			S																	25-14	5.000.000	800.000	0	0	0	0	EPS005	5.000.000	200.000	14-7	5.000.000	3	121.900	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
85	CC	1012483048	CUELLAR LEGUIZAMO HENRY ANDRES	1	0			S	X							X									231001	426.666	68.300	0	0	0	0	EPS008	426.666	17.100	14-7	426.666	3	10.400	CCF22	1.575.790	63.100	1.575.790	0	0	0	0
86	CC	1000469899	ARBOLEDA MEJIA ISABELLA	1	0			S								X									230301	2.301.090	368.200	0	0	0	0	EPS037	2.301.090	92.100	14-7	2.301.090	3	56.100	CCF22	2.301.090	92.100	2.301.090	0	0	0	0
87	CC	1010187944	GUAQUETA GARAVITO IVAN FELIPE	1	0			S								X									231001	3.068.888	491.000	0	0	0	0	EPS010	3.068.666	122.800	14-7	3.068.666	3	74.800	CCF22	3.068.888	122.800	3.068.666	0	0	0	0
88	CC	1018411817	SOZA MINU IVAN LEANDRO	1	0			S	X							X									25-14	424.485	68.000	0	0	0	0	EPS002	424.485	17.000	14-7	424.485	3	10.400	CCF22	875.955	35.100	875.955	0	0	0	0
89	CC	1193462485	BECERRA HURTADO JNDER	1	0			S													X				230301	1.866.667	298.700	0	0	0	0	EPS005	1.866.667	74.700	14-7	1.866.667	3	45.500	CCF22	1.866.667	74.700	1.866.667	0	0	0	0
90	CC	1193462485	BECERRA HURTADO JNDER	1	0			S													X				230301	136.418	21.900	0	0	0	0	EPS005	136.418	5.500	14-7	136.418	3	0	CCF22	135.427	5.500	135.427	0	0	0	0
91	CC	80864294	LOZANO SANCHEZ JAIME ALEXIS	1	0			S								X									230301	4.670.000	747.200	0	0	0	0	EPS017	4.670.000	186.800	14-7	4.670.000	3	113.800	CCF22	4.670.000	186.800	4.670.000	0	0	0	0
92	CC	91366770	QUINTERO GIL JAIR ALEXANDER	1	0			S																	231001	6.000.000	960.000	0	0	30.000	30.000	EPS017	6.000.000	240.000	14-7	6.000.000	3	146.200	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
93	CC	80035889	RODRIGUEZ VIVAS JAIRO FABIAN	1	0			S								X									25-14	2.300.000	368.000	0	0	0	0	EPS005	2.300.000	92.000	14-7	2.300.000	3	56.100	CCF22	2.300.000	92.000	2.300.000	0	0	0	0
94	CC	1033687102	TOLOSA RIVERA JAVIER ANDRES	1	0			S								X									230301	2.045.455	327.300	0	0	0	0	EPS002	2.045.455	81.900	14-7	2.045.455	3	49.800	CCF22	2.045.455	81.900	2.045.456	0	0	0	0
95	CC	1016030560	CORONADO LARA JEFERSON SMITH	1	0			S										X							230301	1.423.500	227.800	0	0	0	0	EPS005	1.423.500	57.000	14-7	1.423.500	3	0	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
96	CC	1115893587	RODRIGUEZ BERNAL JEINSON ANDRES	1	0			S								X									230301	3.527.727	564.500	0	0	0	0	EPS002	3.527.727	141.200	14-7	3.527.727	3	88.000	CCF34	3.527.727	141.200	3.527.727	0	0	0	0
97	CC	1070624193	CANDIA ORTEGA JEISON ANDRES	1	0			S								X									230301	2.770.908	443.400	0	0	0	0	EPS002	2.770.908	110.900	14-7	2.770.908	3	67.500	CCF22	2.770.908	110.900	2.770.908	0	0	0	0
98	CC	9085917?	CAMPOS GALINDO JEISON JAIR	1	0			S	X							X									230201	430.303	68.900	0	0	0	0	EPS005	430.303	17.300	14-7	430.303	3	10.500	CCF22	1.154.860	46.200	1.154.860	0	0	0	0
99	CC	1075248955	PASCUAS ANDRADE JEISSON FERNANDO	1	0			S																	230301	2.416.667	386.700	0	0	0	0	EPS037	2.416.667	96.700	14-7	2.416.667	3	58.900	CCF22	2.416.667	96.700	2.416.667	0	0	0	0
100	CC	1075248955	PASCUAS ANDRADE JEISSON FERNANDO	1	0			S													L				230301	83.333	13.400	0	0	0	0	EPS037	83.333	3.400	14-7	83.333	3	0	CCF22	83.333	3.400	83.333	0	0	0	0
101	CC	1033776192	OSORIO AMESQUITA JEISSON	1	0			S								X									231001	1.766.182	282.600	0	0	0	0	EPS017	1.766.182	70.700	14-7	1.766.182	3	43.100	CCF22	1.766.182	70.700	1.766.182	0	0	0	0
102	CC	79923843	ROJAS ESTUPIÑAN JEISSON	1	0			S								X									230301	1.927.636	308.500	0	0	0	0	EPS008	1.927.636	77.200	14-7	1.927.636	3	47.000	CCF22	1.927.636	77.200	1.927.635	0	0	0	0
103	CC	53153352	CAICEDO JENNIFER ASTRID	1	0			N								X									230301	12.953.850	2.072.700	0	0	64.800	64.800	EPS005	12.953.850	1.619.300	14-7	12.953.850	3	315.600	CCF22	12.953.850	518.200	12.953.850	259.100	388.700	0	0
104	CC	1022406442	CHACON TORRES JESSICA TATIANA	1	0			S								X									230301	3.156.363	505.100	0	0	0	0	EPS010	3.156.363	126.300	14-7	3.156.363	3	76.900	CCF22	3.156.363	126.300	3.156.363	0	0	0	0
105	CC	1093887051	PUENAYAN QUICENO JESUS ALBERTO	1	0			S								X									230301	2.514.480	402.400	0	0	0	0	EPS008	7.514.480	100.600	14-7	7.514.480	3	61.300	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
106	CC	80544134	VARGAS ALONSO JESUS ALBERTO	1	0			S								X									230201	2.868.666	458.900	0	0	0	0	EPS037	2.868.666	114.800	14-7	2.868.666	3	69.900	CCF22	2.868.666	114.800	2.868.666	0	0	0	0
107	CC	52831099	TABARES TELLEZ JEYMMY JOHANNA	1	0			S								X									230201	4.068.666	651.000	0	0	0	0	EPS008	4.068.666	162.800	14-7	4.068.666	3	99.200	CCF22	4.068.666	162.800	4.068.666	0	0	0	0
108	CC	1013652223	CARDENAS HEREDIRA JHOAN SEBASTIAN	1	0			S	X							X									230201	801.999	128.400	0	0	0	0	EPS001	801.999	32.100	14-7	801.999	3	19.600	CCF22	2.218.003	88.800	2.218.003	0	0	0	0
109	CC	1000974498	GALLEGO RIOS JHOAN ESTIBEN	1	0			S	X							X									230301	454.667	72.800	0	0	0	0	EPS005	454.667	18.200	14-7	454.667	3	11.100	CCF22	1.404.561	56.200	1.404.561	0	0	0	0
110	CC	86002274	CAREZAS PISCO JHON ALEXANDER	1	0			S								X									230201	3.672.501	587.700	0	0	0	0	EPS005	3.672.501	147.000	14-7	3.672.501	3	89.500	CCF34	3.672.501	147.000	3.672.501	0	0	0	0
111	CC	1052393576	GARCIA ALBARRACIN JHONATAN ANDRES	1	0			S													X				230301	6.000.000	960.000	0	0	30.000	30.000	EPS017	6.000.000	240.000	14-7	6.000.000	3	146.200	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
112	CC	1000125892	LOPEZ TORRES JHONATAN DAVID	1	0			S									X	X							230301	2.068.666	331.000	0	0	0	0	EPS005	2.068.666	82.800	14-7	2.068.666	3	50.400	CCF22	2.068.666	82.800	2.068.666	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	SI
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A - Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.	

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE										INFORMACIÓN NOVEDADES												PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Colmb. Exterior	Economía	IRG	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	PNL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
140	CC	1032476481	BELLO GARAY JUAN DAVID	1	0			S							X										230201	2.656.819	425.100	0	0	0	0	EPS002	2.656.819	106.300	14-7	2.656.819	3	64.800	CCF22	2.656.819	106.300	2.656.819	0	0	0	0
141	TI	1031651014	BERMÚDEZ MUÑOZ JUAN DAVID	1	0			S							X										25-14	1.658.113	265.300	0	0	0	0	EPS037	1.658.113	66.400	14-7	1.658.113	3	40.400	CCF22	1.658.113	66.400	1.658.113	0	0	0	0
142	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S							X										230201	1.633.254	261.400	0	0	0	0	EPS010	1.633.254	65.400	14-7	1.633.254	3	39.800	CCF22	1.633.254	65.400	1.633.254	0	0	0	0
143	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S									X								230201	69.123	11.100	0	0	0	0	EPS010	69.123	2.800	14-7	69.123	3	0	CCF22	69.123	2.800	69.123	0	0	0	0
144	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S									X								230201	138.245	22.200	0	0	0	0	EPS010	138.245	5.600	14-7	138.245	3	0	CCF22	138.245	5.600	138.245	0	0	0	0
145	CC	80198836	YARA TOVAR JUAN DAVID	1	0			S							X										25-14	3.170.455	507.300	0	0	0	0	EPS017	3.170.455	126.900	14-7	3.170.455	3	77.300	CCF22	3.170.455	126.900	3.170.455	0	0	0	0
146	CC	1000513272	ZAPATA MANRIQUE JUAN DIEGO	1	0			S																	230301	1.933.334	309.400	0	0	0	0	EPS017	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
147	CC	1000513272	ZAPATA MANRIQUE JUAN DIEGO	1	0			S													L				230301	66.667	10.700	0	0	0	0	EPS017	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
148	CC	1070967311	ORTIZ SIMBAQUEBA KAREN LORENA	1	0			S							X										231001	1.761.382	281.900	0	0	0	0	EPS037	1.761.382	70.500	14-7	1.761.382	3	43.000	CCF22	1.761.382	70.500	1.761.382	0	0	0	0
149	CC	1005068478	SEPULVEDA VILLAMIZAR KEINNY JHOSELIN	1	0			S	X																230201	2.500.000	400.000	0	0	0	0	EPS005	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
150	CC	1031175190	PEREZ CARDOZO KEVYN ANDRES	1	0			S							K										230301	2.207.908	352.500	0	0	0	0	EPS037	2.207.908	88.200	14-7	2.207.908	3	53.700	CCF22	2.207.908	88.200	2.207.908	0	0	0	0
151	CC	1002926568	QUISOBONY MALES KEVIN JULIAN	1	0			S		X					X										230201	494.667	78.200	0	0	0	0	EPS005	494.667	19.800	14-7	494.667	3	12.100	CCF22	2.290.973	91.700	2.290.973	0	0	0	0
152	CC	1026667815	PAEZ GOMEZ LAURA YURANI	1	0			S							X										230301	5.000.000	800.000	0	0	0	0	EPS017	5.000.000	200.000	14-7	5.000.000	3	121.800	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
153	CC	1030693689	PINZON DUARTE LEIDY LORENA	1	0			S																	25-14	3.000.000	480.000	0	0	0	0	EPS017	3.000.000	120.000	14-7	3.000.000	3	73.100	CCF22	3.000.000	120.000	3.000.000	0	0	0	0
154	CC	1031168358	GARZON TIRANO LEONARDO DAVID	1	0			S							X										230301	1.917.819	306.900	0	0	0	0	EPS005	1.917.819	76.800	14-7	1.917.819	3	46.800	CCF22	1.917.819	76.800	1.917.819	0	0	0	0
155	CC	79717994	GONZALEZ HERRERA LEONARDO	1	0			S																	25-14	2.000.000	320.000	0	0	0	0	EPS005	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
156	CC	1102794851	TORRES VERGEL LISETH ROCIO	1	0			S																	231001	1.525.000	244.000	0	0	0	0	EPS002	1.525.000	61.000	14-7	1.525.000	3	37.200	CCF22	1.525.000	61.000	1.525.000	0	0	0	0
157	CC	52691376	SCARPETTA MAHECHA LITZA MARIA	1	0			S																	230201	1.800.000	288.000	0	0	0	0	EPS017	1.800.000	72.000	14-7	1.800.000	3	43.900	CCF22	1.800.000	72.000	1.800.000	0	0	0	0
158	CC	1090452471	SARKIS ROZO LIZETH CAROLINA	1	0			S																	230301	2.500.000	400.000	0	0	0	0	EPS017	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
159	CC	1061728990	MANQUILLO LAGOS LUCERO MARISOL	1	0			S																	230301	5.694.000	911.100	0	0	28.500	28.500	EPS005	5.694.000	227.800	14-7	5.694.000	3	138.800	CCF14	5.694.000	227.800	5.694.000	0	0	0	0
160	PT	1062643	OVALLES LAMONT LUIS RAFAEL	1	0			S							X										230301	1.879.928	300.800	0	0	0	0	EPS008	1.879.928	75.200	14-7	1.879.928	3	45.800	CCF22	1.879.928	75.200	1.879.928	0	0	0	0
161	CC	1022989189	RUGE ARJONA LUIS ALFREDO	1	0			S																	230201	3.266.667	522.700	0	0	0	0	EPS002	3.266.667	130.700	14-7	3.266.667	3	79.600	CCF22	3.266.667	130.700	3.266.667	0	0	0	0
162	CC	1022989189	RUGE ARJONA LUIS ALFREDO	1	0			S									X								230201	241.715	38.700	0	0	0	0	EPS002	241.715	9.700	14-7	241.715	3	0	CCF22	241.715	9.700	241.715	0	0	0	0
163	CC	1061688775	MARTINEZ ACOSTA LUIS CARLOS	1	0			S					X												230301	9.500.000	1.520.000	0	0	47.500	47.500	EPS005	9.500.000	380.000	14-7	9.500.000	3	731.500	CCF22	9.500.000	380.000	9.500.000	0	0	0	0
164	CC	91215256	LOPEZ FELICIANO LUIS FERNANDO	1	0			S							X										25-14	2.275.000	364.000	0	0	0	0	EPS017	2.275.000	91.000	14-7	2.275.000	3	55.500	CCF22	2.275.000	91.000	2.275.000	0	0	0	0
165	CC	1001041013	PULIDO LATORRE LUISA FERNANDA	1	0			S																	25-14	2.500.000	400.000	0	0	0	0	EPS005	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
166	CC	40340478	LOTE PEÑA LUZ ADRIANA	1	0			S	X								X								230301	435.394	69.700	0	0	0	0	EPS008	435.394	17.500	14-7	435.394	3	10.700	CCF22	1.436.412	57.500	1.436.412	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 196 # 64-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ D.C.	SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD
					EMPLEADOS: 185 / UPC: 0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE										INFORMACIÓN NOVEDADES																PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Colilla	Ingreso	Extranjero	Cotiza en el exterior	Especial	IRP	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
194	CC	1019100559	VILLAFAÑE PORRAS PATRICIA ISABEL	1	0			S								X									230901	6.068.666	971.000	0	0	30.400	30.400	EPS008	6.068.666	242.800	14-7	6.068.666	3	147.900	CCF22	6.068.666	242.800	6.068.665	0	0	0	0
195	CC	1044391395	CORONEL RODRIGUEZ PEDRO ALEXANDER	1	0			S								X									230201	3.491.394	558.700	0	0	0	0	EPS005	3.491.394	139.700	14-7	3.491.394	3	85.100	CCF22	3.491.394	139.700	3.491.394	0	0	0	0
196	CC	1012437605	MARTINEZ ROMERO RAFAEL STEVEN	1	0			S								X									230301	5.041.395	806.700	0	0	0	0	EPS008	5.041.395	201.700	14-7	5.041.395	3	122.900	CCF22	5.041.395	201.700	5.041.395	0	0	0	0
197	CC	1020827956	LEON LEON RAUL EDUARDO	1	0			S								X									231001	2.836.364	453.900	0	0	0	0	EPS005	2.836.364	113.500	14-7	2.836.364	3	69.100	CCF22	2.836.364	113.500	2.836.364	0	0	0	0
198	CC	1073704285	GUIO COY RICARDO	1	0			S								X									230301	2.205.606	352.900	0	0	0	0	EPS008	2.205.606	88.300	14-7	2.205.606	3	53.800	CCF22	2.205.606	88.300	2.205.606	0	0	0	0
199	CC	1073704285	GUIO COY RICARDO	1	0			S									X								230301	72.199	11.600	0	0	0	0	EPS008	72.199	2.900	14-7	72.199	3	0	CCF22	72.199	2.900	72.199	0	0	0	0
200	CC	1077468830	RENTERIA ROMAÑA ROIDER	1	0			S								X									230301	1.923.636	307.600	0	0	0	0	EPS008	1.923.636	77.000	14-7	1.923.636	3	46.900	CCF22	1.923.636	77.000	1.923.636	0	0	0	0
201	CC	1030661108	CARVAJAL CALDERON ROMAL EDUARDO	1	0			S																	230901	3.150.000	504.000	0	0	0	0	EPS002	3.150.000	126.000	14-7	3.150.000	3	76.800	CCF22	3.150.000	126.000	3.150.000	0	0	0	0
202	CC	25662805	CORREA NACHE ROSALINA	1	0			S																	25-14	5.500.000	880.000	0	0	0	0	EPS005	5.500.000	220.000	14-7	5.500.000	3	134.000	CCF22	5.500.000	220.000	5.500.000	0	0	0	0
203	CC	1012385381	ROJAS RICO RUBEN DARIO	1	0			S								X									230301	2.558.303	409.400	0	0	0	0	EPS002	2.558.303	102.400	14-7	2.558.303	3	62.400	CCF22	2.558.303	102.400	2.558.303	0	0	0	0
204	CC	1012385381	ROJAS RICO RUBEN DARIO	1	0			S										X							230301	60.000	9.600	0	0	0	0	EPS002	60.000	2.400	14-7	60.000	3	0	CCF22	60.000	2.400	60.000	0	0	0	0
205	CC	1031156423	GOMEZ FLAUTERO SAMMIR YECID	1	0			S								X									230301	6.268.666	1.003.000	0	0	31.400	31.400	EPS005	6.268.666	250.800	14-7	6.268.666	3	152.800	CCF22	6.268.666	250.800	6.268.666	0	0	0	0
206	CC	1006506006	GALINDO AUCHAMA SAMUEL	1	0			S																	230301	1.423.500	227.800	0	0	0	0	MIN001	1.423.500	57.000	14-7	1.423.500	3	34.700	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
207	CC	1027402923	NINCO URIBE SANTIAGO	1	0			S								X									230301	2.345.454	375.300	0	0	0	0	EPS008	2.345.454	93.900	14-7	2.345.454	3	57.200	CCF22	2.345.454	93.900	2.345.454	0	0	0	0
208	CC	1026258577	MORALES GALINDO SEBASTIAN	1	0			S								X									230201	6.068.666	971.000	0	0	30.400	30.400	EPS005	6.068.666	242.800	14-7	6.068.666	3	147.900	CCF22	6.068.666	242.800	6.068.666	0	0	0	0
209	CC	1022371537	ROBERTO RODRIGUEZ SEBASTIAN	1	0			S								X									231001	4.610.164	737.700	0	0	0	0	EPS005	4.610.164	184.500	14-7	4.610.164	3	112.400	CCF22	4.583.334	183.400	4.583.334	0	0	0	0
210	CC	1022371537	ROBERTO RODRIGUEZ SEBASTIAN	1	0			S									X								231001	938.889	150.300	0	0	0	0	EPS005	938.889	37.600	14-7	938.889	3	0	CCF22	885.790	35.500	885.790	0	0	0	0
211	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S								X									231001	2.137.335	342.000	0	0	0	0	EPS005	2.137.335	85.500	14-7	2.137.335	3	52.100	CCF22	2.137.335	85.500	2.137.335	0	0	0	0
212	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S									X								231001	466.667	74.700	0	0	0	0	EPS005	466.667	0	14-7	466.667	3	0	CCF22	466.667	0	466.667	0	0	0	0
213	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S															L		231001	66.667	10.700	0	0	0	0	EPS005	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
214	CC	80876276	RAMIREZ ORTIZ SERGIO IVAN	1	0			S								X									230901	7.137.332	1.142.000	0	0	35.700	35.700	EPS017	7.137.332	285.500	14-7	7.137.332	3	173.900	CCF22	7.137.332	285.500	7.137.332	0	0	0	0
215	CC	1018418106	OROZCO PEREZ SINDY PAOLA	1	0			S								X									25-14	3.080.000	492.800	0	0	0	0	EPS010	3.080.000	123.200	14-7	3.080.000	3	75.100	CCF22	3.080.000	123.200	3.080.000	0	0	0	0
216	CC	1000123544	ANGARITA CASTELLANOS TATIANA ANDREA	1	0			S								X									230301	951.382	152.300	0	0	0	0	EPS010	951.382	38.100	14-7	951.382	3	23.200	CCF22	951.382	38.100	951.382	0	0	0	0
217	CC	1000123544	ANGARITA CASTELLANOS TATIANA ANDREA	1	0			S															X		230301	866.332	138.700	0	0	0	0	EPS010	866.332	34.700	14-7	866.332	3	0	CCF22	831.294	33.300	831.294	0	0	0	0
218	CC	1000491664	VALENCIA MUÑOZ TATIANA	1	0			S																	25-14	2.000.000	320.000	0	0	0	0	EPS002	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
219	CC	1072322732	PARRA PADILLA THOMAS ALEJANDRO	1	0			S								X									230301	2.121.955	339.800	0	0	0	0	EPS002	2.121.955	84.900	14-7	2.121.955	3	51.700	CCF22	2.121.955	84.900	2.121.955	0	0	0	0
220	CC	1072444863	BOLIVAR ARAQUE VALENTINA	1	0			S																	230301	2.000.000	320.000	0	0	0	0	EPS008	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar : miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **NGEEK SAS**, identificada con **NI** número **900697738**, aportó por **JUAN PABLO MACIAS VARGAS**, identificado(a) con **CC** número **1032363649** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92105001** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

| | | |

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
CC 79906707		GODOY LOPEZ EDGAR ALFONSO	INDEPENDIENTE	PRINCIPAL	CRA QUINTA # 2- 35 MANZANA 21 CASA 208	MOSQUERA-CUNDINAMARCA	8272125	No

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2025-11	2025-11	2000405053	9495008625	I	2025/12/02	2025/12/11	BANCOLOMBIA	9	$444,500

LIQUIDACION DETALLADA DE APORTES

EMPLEADO				NOVEDADES																PENSION				SALUD				CCF				RIESGOS				PARAFISCALES				
No.	Identificación		Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vsp	Codigo	Días	IBC	Aporte	Codigo	Días	IBC	Aporte	Codigo	Días	IBC	Aporte	Codigo	Días	IBC	Aporte	Días	IBC	Aporte	Exonerado SENA e ICBF	Total Aportes
1	CC	79906707	GODOY LOPEZ EDGAR ALFONSO							X											230201	30	$1,423,500	$227,800	EPS005	30	$1,423,500	$170,000	CCF21	30	$1,423,500	$28,500	14-4	30	$1,423,500	$7,500	30	$0	$0	No	$441,800
Total	Afiliados(1)																						$1,423,500	$227,800			$1,423,500	$170,000			$1,423,500	$28,500			$1,423,500	$7,500		$0	$0		$441,800

2025/12/11 04:23 PM

compensar | miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **TSG THE IT EXPERTS SAS**, identificada con **NI** número **900994724**, aportó por **RONALD ALEXANDER CASTAÑEDA OLARTE**, identificado(a) con **CC** número **80195893** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92105012** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

| | | |

COMANDO GENERAL	ENTRADA DE BIENES	
	COMANDO GRAL FFMM	
	CODIGO SOCIEDAD: 2000	
	NIT: 800230729-9	PÁGINA: 1 de 1

CIUDAD : BOGOTÁ D.C.	FECHA : : 12.12.2025	HORA : 17:51:23
ALMACEN QUE RECIBE : ALMACEN GENERAL RIC		
CONCEPTO DE LA ENTRADA : ENTRADA PONDERABLE CONTRATO 259 COGFM DIADF 2025		

TIPO DE DOCUMENTO : Contab.activo fijo	ACTA No.	REG. AL FOLIO No
PROVEEDOR :	NIT o C.C PROVEEDOR :	
FACTURA No. :	FECHA FACTURA : 12.12.2025	
ENTREGA PARCIAL :	ULTIMA ENTREGA :	
RECIBIDO DE : MY.LOMBANA CARDONA JOSE FRANCISCO	NIT o CC. 14395966	
INFO.ADICIONAL: ENTRADA ACTIVO FIJO INGRESADO COMO PONDERABLE DEL CONTRATO NO 259 COGFM DIADF 2025 MEDIANTE CARTA PONERABLE		

NUM.ACTIVO	No.DOCUM	DESC. ELEMENTO	No. SERIE	CAN	U.M	NUMERO INVENTARIO	COSTO HIST.	DEP. ACUM.	V.N. CONTABLE
163500068922	3000012395	COMPUTADOR		1	UN	80040200000000000000179916	21.441.865,52	0,00	21.441.865,52
TOTAL				1			21.441.865,52	0,00	21.441.865,52

IMPUTACION CONTABLE

COD CONTABLE	NOMBRE CUENTA	DEBITO	CREDITO
1635040020	Equipos y Materiales de Computación	21.441.865,52	0,00
4428300010	Bienes procedentes sector privado	0,00	21.441.865,52
TOTAL		21.441.865,52	21.441.865,52

VALORIZACIONES Y PROVISIONES

NUMERO ACTIVO	DESCRIPCION DEL ACTIVO	VALORIZACION	PROVISION
TOTAL		0,00	0,00

ALMACENISTA QUE RECIBE	NOMBRE Y FIRMA DE QUIEN ENTREGA
SS CLAVIJO BUITRAGO DEIBY LEONARDO C.C 1069727968	MY.LOMBANA CARDONA JOSE FRANCISCO C.C 14395966

UT 273COGFM H&Y 2025 - NIT 901988423-0
Responsable de IVA
CL 98 # 70 - 91 OF 202 203, Bogotá, D.C., Bogotá D.C.,
jbravo@heimcore.com.co
Tel: +573176384129

FACTURA ELECTRÓNICA DE VENTA

FV5

Fecha de creación: 12/12/2025
Fecha de vencimiento: 11/01/2026

Cliente: COMANDO GENERAL DE LAS FUERZAS MILITARES
NIT: 800230729-9
Dirección: Bogotá, D.C. Bogotá D.C. AV DORADO CAN CRR 54 N 26- 25
Teléfono: 3006917716
Email: slifnacion.facturaelectronica@minhacienda.gov.co

Moneda: COP

ID	Ítem	Unidad de medida	Cantidad	Precio	Descuento	Impuesto	Subtotal
1	**SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$387.700.000		-	$387.700.000

Trescientos ochenta y siete millones setecientos mil pesos

Total de líneas: 1

Términos y condiciones:
Este documento se asimila en todos sus efectos a una letra de cambio de conformidad con el Art. 774 del código de comercio. Autorizo que en caso de incumplimiento de esta obligación sea reportado a las centrales de riesgo, se cobraran intereses por mora.

Notas:
#$15-01-02-000; contrato259; facturacionciadf@cgfm.mil.co

Subtotal	$387.700.000
Total a pagar	**$387.700.000**

Moneda: COP
Generado: 2025-12-12 10:19:36-05:00
Validación DIAN: 2025-12-12 10:20:37-05:00
Tipo de factura: FACTURA ELECTRÓNICA DE VENTA
Tipo de operación: Estándar
Proveedor tecnológico: Soluciones Alegra S.A.S
Software: Alegra - NIT 900.559.088-2

CUFE: eda4e3b9c8c9ef89a2790b4bc2a880903d5a445bb5bad720750d50c55bc162751968e14c50239a1ebd72288a0e7d5da9

Autorización de numeración de facturación N°18764100548263 de 2025-10-24 Modalidad Factura Electrónica Desde N° FV1 hasta FV100 con vigencia hasta 2027-10-24

Representación gráfica de factura de venta electrónica

UT 273COGFM H&Y 2025 - NIT 901988423-0
Responsable de IVA
CL 98 # 70 - 91 OF 202 203, Bogotá, D.C., Bogotá D.C.,
jbravo@heimcore.com.co
Tel: +573176384129

FACTURA ELECTRÓNICA DE VENTA
FV6

Fecha de creación: 12/12/2025
Fecha de vencimiento: 11/01/2026

Cliente: COMANDO GENERAL DE LAS FUERZAS MILITARES
NIT: 800230729-9
Dirección: Bogotá, D.C. Bogotá D.C. AV DORADO CAN CRR 54 N 26- 25
Teléfono: 3006917716
Email: siifnacion.facturaelectronica@minhacienda.gov.co

Moneda: COP

ID	Ítem	Unidad de medida	Cantidad	Precio	Descuento	Impuesto	Subtotal
1	**1.1 SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$237.780.000		-	$237.780.000
2	**1.2 SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$189.820.000		-	$189.820.000
3	**1.3 SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$151.664.000		-	$151.664.000
4	**1.4 SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$67.540.000		-	$67.540.000
5	**1.5 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo**	Servicio	1	$47.069.000		-	$47.069.000
6	**1.6 SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$13.642.000		-	$13.642.000
7	**1.7 SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)**	Servicio	1	$380.000.000		-	$380.000.000

Mil ochenta y siete millones quinientos quince mil pesos

Total de líneas: 7

Términos y condiciones:
Este documento se asimila en todos sus efectos a una letra de cambio de conformidad con el Art. 774 del código de comercio. Autorizo que en caso de incumplimiento de esta obligación sea reportado a las centrales de riesgo, se cobraran intereses por mora.

Notas:
#$15-01-02-000; contrato259; facturaciondiadf@cgfm.mil.co

Moneda: COP
Generado: 2025-12-12 13:39:48-05:00
Validación DIAN: 2025-12-12 13:40:48-05:00
Tipo de factura: FACTURA ELECTRÓNICA DE VENTA
Tipo de operación: Estándar
Proveedor tecnológico: Soluciones Alegra S.A.S
Software: Alegra - NIT 900.559.088-2

CUFE: ebf6de9d8a8fab0d82a380a1bc297316b718d43897889b361e71b6b623bc9e83c2d78b4f787a20f16d4865abfd310817

Autorización de numeración de facturación N°18764100548263 de 2025-10-24 Modalidad Factura Electrónica Desde N° FV1 hasta FV100 con vigencia hasta 2027-10-24

Representación gráfica de factura de venta electrónica

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: Entrega de Ponderables – Contrato No. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del Contrato No. 259COGFM DIADF 2025, la Unión Temporal UT273COGFM H&Y 2025, en calidad de Contratista, manifiesta formalmente su compromiso de garantizar la correcta prestación del Servicio de Suscripción WAF – Lote No. 5.

En atención al requerimiento de entrega de los ponderables correspondientes, se informa que se ha realizado la entrega efectiva de los compromisos establecidos, conforme se detalla a continuación:

No.	DESCRIPCIÓN DEL BIEN O SERVICIO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
1	**El contratista ofrece sin costo adicional:** Terminal para administración y gestión de la solución de seguridad que debe incluir como mínimo Intel® Core™ Ultra 7 265KF, Windows 11 Pro, NVIDIA® GeForce RTX™ 5080, 32 GB DDR5, SSD de 2 TB, con periféricos incluidos y 02 dispositivos de visualización de 25" que permitan visualización y monitoreo de datos críticos, sin que este ofrecimiento genere costo adicional para la entidad.	1	$ 21,441,865.52	$ 21,441,865.52

compensar | miplanilla.com

REPORTE RESUMEN DE PAGO

Información básica de la planilla

Empresa:	HEIMCORE SAS	**NIT:**	900425697
Tipo Planilla:	E	**Periodo liquidación Pensiones:**	octubre 2025
Sucursal o Dependencia:	PRINCIPAL	**Periodo liquidación Salud:**	noviembre 2025
Número de Radicación:	91346758	**Total a pagar:**	$281,618,700
Fecha de vencimiento:	26/11/2025	**Total de empleados:**	200
Fecha de Pago:	21/11/2025	**Número de Administradoras:**	25

Detalles del pago

Razón social recaudo:	Compensar OI	**Nit recaudo:**	9998600669427
Descripción:	MIPlanilla.com Pago Proteccion Social	**Medio de Pago:**	Pago Electronico por PSE
Banco:	BANCO DE BOGOTA	**Número Autorización:**	1945289551
Estado de la transacción:	Transacción aprobada		

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
14-11	890903790	ARL SURA	200		$0	$9,801,700
230201	800229739	Proteccion (ING + Proteccion)	50		$0	$40,225,400
230301	800224808	Porvenir	86		$0	$52,828,600
230901	800253055	Skandia Fondo de Pensiones Obligatorias	5		$0	$9,802,100
231001	800227940	Colfondos	27		$0	$25,865,600
25-14	900336004	Administradora Colombiana de Pensiones -	28		$0	$29,453,200
CCF04	890900841	Comfama Caja de Compensacion Fliar	2		$0	$582,200
CCF06	890102002	Combarranquilla Caja de Compensacion Fliar	3		$0	$536,000
CCF13	891190047	Comfaca Caja de Compensacion Fliar	1		$0	$64,000
CCF24	860066942	Compensar Caja de Compensacion Fliar	184		$0	$36,222,900
CCF39	890200106	Cajasan Caja de Compensacion Fliar	1		$0	$64,000
CCF44	891480000	Comfamiliar Risaralda Caja de Compensacion Fliar	2		$0	$134,400
CCF48	800211025	Comfatolima Caja de Compensacion Fliar	1		$0	$64,000
CCF57	890303208	Comfamiliar Andi Comfandi Caja de	2		$0	$224,000
EPS001	830113831	ALIANSALUD EPS S.A.	10		$0	$7,864,700
EPS002	800130907	Salud Total EPS	27		$0	$8,688,100
EPS005	800251440	Sanitas EPS	67		$0	$25,231,900

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
EPS008	860066942	Compensar EPS	37		$0	$7,967,500
EPS010	800088702	EPS Sura	26		$0	$6,949,400
EPS017	830003564	Famisanar EPS Cafam Colsubsidio	23		$0	$4,229,900
EPS037	900156264	Nueva Promotora de Salud - Nueva EPS	8		$0	$996,800
EPS041	900156264	NUEVA E.P.S. S.A. MOV	1		$0	$134,200
MIN001	901037916	Fondo de Solidaridad y Garantía - FOSYGA	1		$0	$57,000
PAICBF	899999239	ICBF Instituto Colombiano de Bienestar Familiar	20		$0	$8,178,900
PASENA	899999034	SENA	20		$0	$5,452,200
						$281,618,700

***Si descontó incapacidades o notas crédito debe informar a la administradora correspondiente los descuentos.**

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL / CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A – Más de 200 cot	YEAPDATA / YEAPDATA	BOGOTÁ, D.C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS001	ALIANSALUD EPS S.A.	830113831-0	2.339.000	0		0		0	0	0	0	2.339.000	5
EPS002	Salud Total EPS	800130907-4	2.122.900	0		0		0	0	0	0	2.122.900	22
EPS005	Sanitas EPS	800251440-6	12.574.800	0		0		0	0	0	0	12.574.800	54
EPS008	Compensar EPS	860066942-7	5.363.200	0		0		0	0	0	0	5.363.200	39
EPS010	EPS Sura	800088702-2	2.302.900	0		0		0	0	0	0	2.302.900	17
EPS017	Famisanar EPS	830003564-7	4.764.500	0		0		0	0	0	0	4.764.500	34
EPS037	Nueva EPS	900156264-2	791.200			0		0	0	0	0	791.200	4
EPSC25	Capresoca EPS	891856000-5	136.500			0		0	0	0	0	136.500	1
EPSC34	Asmet Salud SGP Capital Salud	900298372-3	27.700			0		0	0	0	0	27.700	1
MIN001	Ministerio Sol y Gar Min Salud	901035086-1	292.100			0		0	0	0	0	292.100	2

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230201	Proteccion (ING + Proteccion)	800229739-0	16.226.500	0	0	99.000	99.000	0	0		16.424.500	36
230301	Porvenir	800224808-8	40.910.400	0	0	463.800	463.800	0	0		41.838.000	80
230901	Skandia Pensiones Obligatorias	800253055-2	6.958.700	0	0	121.500	121.500	0	0		7.201.700	8
231001	Colfondos	800227940-6	13.601.600	0	0	283.100	283.100	0	0		14.167.800	20
25-14	Colpensiones	900336004-7	27.126.600	0	0	342.900	342.900	0	0		27.812.400	41

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatorio	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-7	Seguros Bolivar S.A.	860002503-2	15.428.900				15.428.900	0	0	15.428.900			154.289	15.428.900	185

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF14	Comfacauca	891500182-0	253.100	0	0	253.100	2
CCF22	Colsubsidio	860007336-1	25.913.600	0	0	25.913.600	179
CCF34	Cotrem	892000146-3	412.500	0	0	412.500	3
CCF69	Comfacesanare	844003392-8	136.500	0	0	136.500	1

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE

TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS		Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	**CLASE APORTANTE**	**NOMBRE SUCURSAL**	**CÓDIGO**	**DEPARTAMENTO**	**CIUDAD / MUNICIPIO**		
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ. D. C.	BOGOTÁ. D C		SI

DATOS DE LA PLANILLA

PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					185	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

TOTALES PARAFISCALES

Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
SENA				
1.037.700	0	0	1.037.700	5
ICBF				
1.556.800	0	0	1.556.800	5
ESAP				
MEN				

TOTALES POR SUBSISTEMA

Tipo Administradora	No. Administradoras Reportadas	Valor antes de IGE, LMA, IRP y Mora	Total a Pagar
Salud	10	30.714.800	30.714.800
Pensión	5	107.444.400	107.444.400
Riesgos Laborales	1	15.428.900	15.428.900
CCF	4	26.715.700	26.715.700
ESAP	0	0	0
ICBF	1	1.556.800	1.556.800
MEN	0	0	0
SENA	1	1.037.700	1.037.700
TOTALES	22	182.898.300	182.898.300

PAGADA

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE							
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS		Carrera 19B # 84-17 Ofc 403- 404	3154026330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A – Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ, D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119673	$162.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Pensión	Subsistema	Otros subsistemas	Extranjero	IGE	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	COMENTARIOS	Cód. AFP	IBC AFP	Cotización	Voluntario o Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC	1014256751	BETANCOURT BARRERA JESICA ALEJANDRA	1	0			S																	230301	10.500.000	1.680.000	0	0	52.500	52.500	EPS005	10.500.000	420.000	14-7	10.500.000	3	255.800	CCF22	10.500.000	420.000	10.500.000	0	0	0	0
2	CC	80133820	AGUILAR GARCIA ALEX CRISTIAN	1	0			S								X								25-14	3.815.257	610.500	0	0	0	0	EPS005	3.815.257	152.700	14-7	3.815.257	3	99.000	CCF22	3.815.257	152.700	3.815.257	0	0	0	0
3	CC	79627591	AREVALO BUITRAGO ALEXANDER	1	0			S																	25-14	12.953.856	2.072.700	0	0	64.800	64.800	EPS001	12.953.856	1.619.300	14-7	12.953.856	3	518.200	CCF22	12.953.856	518.200	12.953.856	259.100	388.700	0	0
4	CC	52274867	VASQUEZ RODRIGUEZ ALEXANDRA	1	0			S																	25-14	3.500.000	560.000	0	0	0	0	EPS005	3.500.000	140.000	14-7	3.500.000	3	85.300	CCF22	3.500.000	140.000	4.146.667	0	0	0	0
5	CC	52337501	GUTIERREZ DIAZ ANA CRISTINA	1	0			S																	25-14	3.535.333	565.700	0	0	0	0	EPS005	3.535.333	141.500	14-7	3.535.333	3	86.200	CCF22	3.535.333	141.500	3.535.333	0	0	0	0
6	CC	52337501	GUTIERREZ DIAZ ANA CRISTINA	1	0			S								X									25-14	516.130	82.600	0	0	0	0	EPS005	516.130	20.700	14-7	516.130	3	0	CCF22	516.130	20.700	516.130	0	0	0	0
7	CC	52843373	QUINTERO [redacted] ANA ELISA	1	0			S																	231001	7.000.000	1.120.000	0	0	35.000	35.000	EPS [redacted]	7.000.000	280.000	14-7	7.000.000	3	170.600	CCF22	7.000.000	280.000	7.000.000	0	0	0	0
8	CC	1010005905	CAMARGO [redacted] ANA SOFIA	1	0			S	X																230301	2.159.091	345.500	0	0	0	0	E [redacted]	2.159.091	86.400	14-7	2.159.091	3	52.600	CCF22	5.262.336	210.500	5.262.336	0	0	0	0
9	CC	1023976244	MARIN ACELDA [redacted] EI ALEJANDRO	1	0			S	X																230301	454.667	72.800	0	0	0	0	E [redacted]	454.667	18.200	14-7	454.667	3	11.100	CCF22	1.370.628	54.800	1.370.628	0	0	0	0
10	CC	1018509611	CORREDOR T [redacted]	1	0			S								X									230301	2.666.666	427.000	0	0	0	0	E [redacted]	2.666.666	106.700	14-7	2.666.666	3	65.100	CCF22	2.668.666	106.800	2.668.666	0	0	0	0
11	CC	1000954518	MAI DONADO BO [redacted]	1	0			S								X									230701	2.668.666	427.000	0	0	0	0	E [redacted]	2.668.666	106.700	14-7	2.668.666	3	65.100	CCF22	2.668.666	106.800	2.668.666	0	0	0	0
12	CC	1018473110	MISSE AYA [redacted] RES FELIPE	1	0			S																	230201	1.933.333	309.400	0	0	0	0	E [redacted]	1.933.333	77.400	14-7	1.933.333	3	47.100	CCF22	1.933.333	77.400	1.933.333	0	0	0	0
13	CC	1018473110	MISSE AYA [redacted] RES FELIPE	1	0			S																	230201	72.166.666	11.500.000	0	0	0	0	E [redacted]	72.166.666	2.900.000	14-7	72.166.666	3	0	CCF22	72.166.666	2.900.000	72.166.666	0	0	0	0
14	CC	1098618398	RINCON ORT [redacted] RES MAURICIO	1	0			S																	230201	7.000.000	1.120.000	0	0	35.000	35.000	EPS010	7.000.000	280.000	14-7	7.000.000	3	170.600	CCF22	7.000.000	280.000	7.000.000	0	0	0	0
15	CC	1106890585	TAPIAS PORTE [redacted] RES MAURICIO	1	0			S								X									230301	4.437.334	771.500	0	0	0	0	EPS008	4.437.334	177.500	14-7	4.437.334	3	108.100	CCF22	4.437.334	177.500	4.437.334	0	0	0	0
16	CC	1015415552	ARAQUE ME [redacted] RES FELIPE	1	0			S								X									230301	11.066.666	1.771.000	0	0	55.400	55.400	EPS008	11.066.666	442.600	14-7	11.066.666	3	269.300	CCF22	11.066.666	442.600	11.066.666	0	0	0	0
17	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	0			S								X									230301	737.332	118.000	0	0	0	0	EPS008	737.332	29.500	14-7	737.332	3	18.000	CCF22	737.332	29.500	737.332	0	0	0	0
18	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	0			S									X								230301	1.395.464	223.300	0	0	0	0	EPS008	1.395.464	55.900	14-7	1.395.464	3	0	CCF22	1.395.464	55.900	1.395.464	0	0	0	0
19	CC	1014181337	CUBILLOS RAMIREZ ANGEL MATEO	1	0			S																L	230301	66.667	10.700	0	0	0	0	EPS008	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
20	CC	53040273	GIL VARGAS ANGELA MARCELA	1	0			S																	231001	11.000.000	1.760.000	0	0	55.000	55.000	EPS001	11.000.000	440.000	14-7	11.000.000	3	269.000	CCF22	11.000.000	440.000	11.000.000	0	0	0	0
21	CC	1090364789	LOPEZ QUINTERO ANTONY FERNEY	1	0			S								X									230201	1.729.718	276.800	0	0	0	0	EPS005	1.729.718	69.200	14-7	1.729.718	3	42.200	CCF22	1.729.718	69.200	1.729.718	0	0	0	0
22	CC	34555976	TERAN ESTUPIÑAN BEATRIZ EUGENIA	1	0			S																	25-14	3.600.000	576.000	0	0	0	0	EPS010	3.600.000	144.000	14-7	3.600.000	3	87.700	CCF22	3.600.000	144.000	3.600.000	0	0	0	0
23	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	0			S								X									230201	1.637.842	262.100	0	0	0	0	EPS008	1.637.842	65.600	14-7	1.637.842	3	39.900	CCF22	1.637.842	65.600	1.637.842	0	0	0	0
24	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	0			S																	230201	65.999	10.600	0	0	0	0	EPS008	65.999	2.700	14-7	65.999	3	0	CCF22	65.999	2.700	65.999	0	0	0	0
25	CC	1012456851	TOVAR FONSECA BEIRO FERNEY	1	0			S																L	230201	53.333	8.500	0	0	0	0	EPS008	53.333	2.200	14-7	53.333	3	0	CCF22	53.333	2.200	53.333	0	0	0	0
26	CC	1110172102	PEDRAZA MENDOZA BENJAMIN	1	0			S								X									230301	1.741.393	278.700	0	0	0	0	EPS017	1.741.393	69.700	14-7	1.741.393	3	42.500	CCF22	1.741.393	69.700	1.741.393	0	0	0	0
27	CC	1000227184	CARDOZO RUBIANO BRAYAN LEONARDO	1	0			S	X							X									231001	811.150	129.800	0	0	0	0	EPS008	811.150	32.500	14-7	811.150	3	19.800	CCF22	1.135.392	45.500	1.135.392	0	0	0	0
28	CC	80180405	MARTINEZ CRUZ CARLOS ANDRES	1	0			S								X									230301	9.214.080	1.474.300	0	0	46.100	46.100	EPS005	9.214.080	368.600	14-7	9.214.080	3	224.500	CCF22	8.000.000	320.000	8.000.000	0	0	0	0
29	CC	1118546521	VEGA CARDENAS CARLOS ANDRES	1	0			S								X									230301	3.412.499	546.000	0	0	0	0	EPS025	3.412.499	136.500	14-7	3.412.499	3	83.200	CCF69	3.412.499	136.500	3.412.499	0	0	0	0
30	CC	1012448626	MORENO CRUZ CESAR SANTIAGO	1	0			S																	230201	2.000.000	320.000	0	0	0	0	EPS005	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
31	CC	1030652679	MACIAS BLANCO CHRISTOPHER	1	0			S								X									231001	4.653.408	744.500	0	0	0	0	EPS002	4.653.408	186.200	14-7	4.653.408	3	113.400	CCF22	4.653.408	186.200	4.653.408	0	0	0	0
32	CC	1072340471	BELEÑO JARAMILLO CLAUDIA MIREYA	1	0			S								X									230201	2.234.181	357.500	0	0	0	0	EPS002	2.234.181	89.400	14-7	2.234.181	3	54.500	CCF22	2.234.181	89.400	2.234.181	0	0	0	0
33	CC	39573802	LONDOÑO GIL CLAUDIA YANET	1	0			S																	231001	1.500.000	240.000	0	0	0	0	EPS002	1.500.000	60.000	14-7	1.500.000	3	36.600	CCF22	1.500.000	60.000	1.500.000	0	0	0	0
34	CC	1033644252	DIAZ ROJAS CRISTIAN CAMILO	1	0			S								X									230301	2.391.877	382.800	0	0	0	0	EPS017	2.391.877	95.700	14-7	2.391.877	3	58.300	CCF22	2.391.877	95.700	2.391.877	0	0	0	0
35	CC	1015455880	GALINDO CASTRO CRISTIAN CAMILO	1	0			S								X									230201	2.585.227	413.700	0	0	0	0	EPS017	2.585.227	103.500	14-7	2.585.227	3	63.000	CCF22	2.585.227	103.500	2.585.227	0	0	0	0
36	CC	1012401928	GUERRERO REVES CRISTIAN CAMILO	1	0			S								X									230301	2.887.998	462.100	0	0	0	0	EPS008	2.887.998	115.600	14-7	2.887.998	3	70.400	CCF22	2.887.998	115.600	2.887.998	0	0	0	0
37	CC	1016064582	ROA GUEVARA CRISTIAN LEONARDO	1	0			S								X									231001	7.307.301	1.168.700	0	0	36.600	36.600	EPS008	7.307.301	292.300	14-7	7.307.301	3	178.100	CCF22	7.307.301	292.300	7.307.301	0	0	0	0
38	CC	1000364348	DELIS MARTINEZ DANIEL ALEJANDRO	1	0			S																	25-14	7.500.000	1.200.000	0	0	37.500	37.500	EPS005	7.500.000	300.000	14-7	7.500.000	3	182.700	CCF22	7.500.000	300.000	7.500.000	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO
NI	900311748-1	YEAPDATA SAS		Carrera 198 # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	EXONERADO PAGO PARAFISCALES Y SALUD
SUCURSAL	A – Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					185	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE								INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES			CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Colom. Labor. Exterior	IRO	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	VTE	IRL	COR	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
39	CC	1019132792	FONSECA CELY DANIEL FELIPE	1	0		S																		230301	2.000.000	320.000	0	0	0	0	EPS002	2.000.000	90.000	14-7	2.000.000	3	48.300	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
40	CC	1036501222	GONZALEZ AVIRAMA DANIEL	1	0		S								x										25-14	2.984.546	477.600	0	0	0	0	EPS005	2.984.546	119.400	14-7	2.984.546	3	72.900	CCF22	2.984.546	119.400	2.984.546	0	0	0	0
41	CC	1015444147	RIVERA PADILLA DANIEL HUMBERTO	1	0		S								x										230301	1.782.423	285.200	0	0	0	0	EPS017	1.782.423	71.300	14-7	1.782.423	3	43.500	CCF22	1.782.423	71.300	1.782.423	0	0	0	0
42	CC	1015444147	RIVERA PADILLA DANIEL HUMBERTO	1	0		S									x									230301	106.667	17.100	0	0	0	0	EPS017	106.667	0	14-7	106.667	3	0	CCF22	106.667	0	106.667	0	0	0	0
43	CC	1000585674	GOMEZ QUIROGA DANIELA	1	0		S								x										230201	2.288.000	366.100	0	0	0	0	EPS037	2.288.000	91.600	14-7	2.288.000	3	55.900	CCF22	2.288.000	91.600	2.288.000	0	0	0	0
44	CC	79746091	AVELLA ROJAS DANNY RAFAEL	1	0		S								x										230201	2.868.586	427.000	0	0	0	0	EPS008	2.868.586	106.800	14-7	2.868.586	3	86.100	CCF22	2.868.666	108.800	2.868.666	0	0	0	0
45	CC	1075664087	GUAVITA MORENO DAVID LEONARDO	1	0		S								x										25-14	1.916.364	306.700	0	0	0	0	EPS008	1.916.364	76.700	14-7	1.916.364	3	46.700	CCF22	1.916.364	76.700	1.916.364	0	0	0	0
46	CC	1027944356	SIERRA PEREZ DAVID MAURICIO	1	0		S									x									25-14	5.000.000	800.000	0	0	0	0	EPS008	5.000.000	200.000	14-7	5.000.000	3	121.800	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
47	CC	1032492909	SILVA RUEDA JUAN SANTIAGO	1	0		S	x																	230301	1.535.078	245.600	0	0	0	0	EPS008	1.535.078	61.400	14-7	1.535.078	3	37.400	CCF22	1.933.078	77.400	1.933.078	0	0	0	0
48	CC	1079033866	CHOLO BELTRAN DEIBYS JAIR	1	0		S																		230301	4.185.333	669.700	0	0	0	0	EPS037	4.185.333	167.500	14-7	4.185.333	3	102.000	CCF22	4.185.333	167.500	4.185.333	0	0	0	0
49	CC	1079033866	CHOLO BELTRAN DEIBYS JAIR	1	0		S																	L	230301	133.333	21.400	0	0	0	0	EPS037	133.333	5.400	14-7	133.333	3	0	CCF22	133.333	5.400	133.333	0	0	0	0
50	CC	52756859	ZAMBRANO AREVALO NANCY MARISELLA	1	0		S	x																	230301	628.485	100.600	0	0	0	0	EPS008	628.485	25.100	14-7	628.485	3	15.400	CCF22	1.665.654	66.600	1.665.654	0	0	0	0
51	CC	1018064697	PLAZAS MILLAN JUAN ALEJANDRA	1	0		S																		231001	6.500.000	1.040.000	0	0	32.500	32.500	EPS037	6.500.000	260.000	14-7	6.500.000	3	158.400	CCF22	6.500.000	260.000	6.500.000	0	0	0	0
52	CC	53054585	MARTIN CASTILLO [illegible]	1	0		S																		230301	2.500.000	400.000	0	0	0	0	EPS005	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
53	CC	1019603233	RUEDA VASQUEZ DIEGO ALEJANDRO	1	0		S																		230301	1.620.000	259.200	0	0	0	0	EPS048	1.620.000	64.800	14-7	1.620.000	3	39.500	CCF22	1.620.000	64.800	1.620.000	0	0	0	0
54	CC	80807723	RODRIGUEZ MORA DIEGO ARMANDO	1	0		S								x										230201	7.715.900	1.234.600	0	0	38.600	38.600	EPS017	7.715.900	308.700	14-7	7.715.900	3	188.000	CCF22	7.715.900	308.700	7.715.900	0	0	0	0
55	CC	1014197739	RODRIGUEZ MORA DIEGO EDISON	1	0		S								x										230201	4.401.138	704.200	0	0	0	0	EPS008	4.401.138	176.100	14-7	4.401.138	3	107.300	CCF22	4.401.138	176.100	4.401.138	0	0	0	0
56	CC	1014197739	RODRIGUEZ MORA DIEGO EDISON	1	0		S																	L	230201	150.000	24.000	0	0	0	0	EPS008	150.000	6.000	14-7	150.000	3	0	CCF22	150.000	6.000	150.000	0	0	0	0
57	CC	1019462866	LOPEZ CASTELLANOS DIEGO	1	0		S								x										230301	3.528.409	564.600	0	0	0	0	EPS002	3.528.409	141.200	14-7	3.528.409	3	88.000	CCF22	3.528.409	141.200	3.528.409	0	0	0	0
58	CC	1033800276	CASTILLO CARDENAS DUBAN	1	0		S								x										230301	3.839.062	614.300	0	0	0	0	EPS005	3.839.062	153.600	14-7	3.839.062	3	93.800	CCF22	3.839.062	153.600	3.839.062	0	0	0	0
59	CC	1012437850	GARRIDO CRIOLLO DUVAN ALEXIS	1	0		S								x										230301	2.001.999	320.400	0	0	0	0	EPS037	2.001.999	80.100	14-7	2.001.999	3	48.800	CCF22	2.001.999	80.100	2.001.999	0	0	0	0
60	CC	1012437850	GARRIDO CRIOLLO DUVAN ALEXIS	1	0		S																	L	230301	66.667	10.700	0	0	0	0	EPS037	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
61	CC	1032438764	ROMERO GAITAN EDGAR DANIEL	1	0		S								x										25-14	166.667	26.700	0	0	0	0	EPS008	166.667	6.700	14-7	166.667	3	4.100	CCF22	166.667	6.700	166.667	0	0	0	0
62	CC	1032438764	ROMERO GAITAN EDGAR DANIEL	1	0		S									x									25-14	666.700	106.700	0	0	0	0	EPS008	666.700	26.700	14-7	666.700	3	0	CCF22	666.700	26.700	666.700	0	0	0	0
63	CC	1032438764	ROMERO GAITAN EDGAR DANIEL	1	0		S									x									25-14	3.333.333	533.400	0	0	0	0	EPS008	3.333.333	133.400	14-7	3.333.333	3	0	CCF22	3.333.333	133.400	3.333.333	0	0	0	0
64	CC	1032438764	ROMERO GAITAN EDGAR DANIEL	1	0		S									x									25-14	500.000	80.000	0	0	0	0	EPS008	500.000	20.000	14-7	500.000	3	0	CCF22	500.000	20.000	500.000	0	0	0	0
65	CC	79597751	MELO GUTIERREZ EDGARD ALIRIO	1	0		S								x										25-14	2.300.000	368.000	0	0	0	0	EPS008	2.300.000	92.000	14-7	2.300.000	3	56.400	CCF22	2.300.000	92.000	2.300.000	0	0	0	0
66	CC	34561033	MARTINEZ LATORRE EDNNA CONSTANZA	1	0		N								x										25-14	12.953.850	2.072.700	0	0	64.800	64.900	EPS005	12.953.850	518.200	14-7	12.953.850	3	315.600	CCF22	12.953.850	518.200	12.953.850	259.100	388.700	0	0
67	CC	11256295	GUCHUVO HERNANDO EDUAR FERNANDO	1	0		S	x																	230301	5.383.334	861.400	0	0	0	0	EPS005	5.383.334	215.400	14-7	5.383.334	3	131.200	CCF22	5.383.334	215.400	5.383.334	0	0	0	0
68	CC	80492906	GAMBOA GONZALEZ EDUARDO	1	0		S								x										230301	1.835.700	293.800	0	0	0	0	EPS017	1.835.700	73.500	14-7	1.835.700	3	44.800	CCF22	1.835.700	73.500	1.835.700	0	0	0	0
69	CC	80155051	GUARQUIN RODRIGUEZ EDWIN ALFONSO	1	0		S																		25-14	2.000.000	320.000	0	0	0	0	EPS017	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
70	CC	79707532	MEDINA CORREA ELKIN MANUEL	1	0		S																		25-14	1.933.334	309.400	0	0	0	0	EPS017	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
71	CC	79707532	MEDINA CORREA ELKIN MANUEL	1	0		S																	L	25-14	66.667	10.700	0	0	0	0	EPS017	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
72	CC	80778648	RIVERO RODRIGUEZ ELKIN	1	0		S								x										230301	2.375.835	380.300	0	0	0	0	EPS010	2.375.835	95.100	14-7	2.375.835	3	57.900	CCF22	2.376.835	95.100	2.376.835	0	0	0	0
73	CC	1024492097	VANEGAS AREVALO FAUSTO CAMILO	1	0		S																		231101	11.010.773	1.761.800	0	0	55.100	55.100	EPS010	11.010.773	440.500	14-7	11.010.773	3	268.300	CCF22	11.010.773	440.500	11.010.773	0	0	0	0
74	CC	1056031160	CASTELLANOS ALARCON FERNEY ALEJANDRO	1	0		S																	x	25-14	4.829.954	772.800	0	0	24.200	24.200	EPS008	4.829.954	193.200	14-7	4.829.954	3	0	CCF22	4.255.030	170.300	4.255.030	0	0	0	0
75	CC	1056031160	CASTELLANOS ALARCON FERNEY ALEJANDRO	1	0		S																		25-14	3.354.214	536.700	0	0	16.800	16.800	EPS008	3.354.214	134.200	14-7	3.354.214	3	81.800	CCF22	3.354.214	134.200	3.354.214	0	0	0	0
76	CC	1022376015	URIZA CAMARGO FRANCISCO JAVIER	1	0		S	x																	231001	733.334	117.400	0	0	0	0	EPS010	733.334	29.400	14-7	733.334	3	17.900	CCF22	1.134.246	45.400	1.134.246	0	0	0	0
77	CC	1022376015	URIZA CAMARGO FRANCISCO JAVIER	1	0		S										x								231001	214.259	34.300	0	0	0	0	EPS010	214.259	8.600	14-7	214.259	3	0	CCF22	214.259	8.600	214.259	0	0	0	0
78	CC	1022376015	URIZA CAMARGO FRANCISCO JAVIER	1	0		S											x							231001	350.488	56.100	0	0	0	0	EPS010	350.488	14.100	14-7	350.488	3	0	CCF22	463.713	18.600	463.713	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO
NI	900311748-1	YEAPDATA SAS		Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	EXONERADO PAGO PARAFISCALES Y SALUD
SUCURSAL	A – Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ, D.C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE										INFORMACIÓN NOVEDADES																PENSIÓN						SALUD			RIESGOS LABORALES			CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Colombiano	Extranjero	Exterior	Salario Integral	Dependiente	ING	RET	TDE	TAE	TDP	TAP	VSP	SLN	IGE	LMA	VAC	AVP	VCT	IRL	DIAS COTIZADOS	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
79	CC	1022376015	URIZA CAMARGO FRANCISCO JAVIER	1	D			S									X							230301	200.279	32.100	0	0	0	0	EPS010	200.279	8.100	14-7	200.279	3	0	CCF22	259.483	10.400	259.483	0	0	0	0
80	CC	1030649824	POBLADOR NAVAS FREED ALEXANDER	1	D			S	X						X									230301	578.545	92.600	0	0	0	0	EPS010	578.545	23.200	14-7	578.545	3	14.100	CCF22	1.974.641	79.000	1.974.641	0	0	0	0
81	CC	1115743751	CARVAJAL MANCHEGO GERMAN ALEXANDER	1	D			S							X									230301	2.006.666	321.100	0	0	0	0	EPS002	2.006.666	80.300	14-7	2.006.666	3	48.900	CCF22	2.006.666	80.300	2.006.666	0	0	0	0
82	CC	1115743751	CARVAJAL MANCHEGO GERMAN ALEXANDER	1	D			S								X								230301	71.345	11.500	0	0	0	0	EPS002	71.345	2.900	14-7	71.345	3	0	CCF22	71.345	2.800	71.345	0	0	0	0
83	CC	1032415420	SOSA MORE[illegible] MARTIN[illegible]	1	D			S																230301	9.000.000	1.440.000	0	0	45.000	45.000	EPS005	9.000.000	360.000	14-7	9.000.000	3	216.000	CCF22	9.000.000	360.000	9.000.000	0	0	0	0
84	CC	52714859	BARRAMON LOP[illegible] ANNA CRISTINA	1	D			S																25-14	5.000.000	800.000	0	0	0	0	EPS005	5.000.000	200.000	14-7	5.000.000	3	121.800	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
85	CC	1012463048	CUELLAR LEGU[illegible] HENRY ANDRES	1	D			S		X														230301	426.666	68.300	0	0	0	0	EPS002	426.666	17.100	14-7	426.666	3	10.400	CCF22	1.575.790	63.100	1.575.790	0	0	0	0
86	CC	1000469859	ARBOLEDA[illegible] ISABELLA	1	D			S																230301	2.301.099	368.200	0	0	0	0	EPS[illegible]	2.301.099	92.100	14-7	2.301.099	3	56.100	CCF22	2.301.099	92.100	2.301.099	0	0	0	0
87	CC	1010187944	GUAQUETA G[illegible] IVAN FELIPE	1	D			S																231001	3.068.666	491.000	0	0	0	0	EPS[illegible]	3.068.666	122.800	14-7	3.068.666	3	74.800	CCF22	3.068.666	122.800	3.068.666	0	0	0	0
88	CC	1018411812	SOZA MIN[illegible] LEANDRO	1	D			S	X															25-14	424.485	67.900	0	0	0	0	E[illegible]	424.485	16.900	14-7	424.485	3	10.400	CCF22	875.955	35.100	875.955	0	0	0	0
89	CC	1193467485	BECERRA[illegible] JAIDER	1	D			S																230301	1.866.667	298.700	0	0	0	0	[illegible]	1.866.667	[illegible]	14-7	1.866.667	3	45.900	CCF22	1.866.667	74.700	1.866.667	0	0	0	0
90	CC	1193482485	BECERRA[illegible]	1	D			S							X									230301	135.421	21.700	0	0	0	0	[illegible]	135.418	[illegible]	14-7	135.418	3	0	CCF22	135.427	5.400	135.427	0	0	0	0
91	CC	80864294	LOZANO SA[illegible]	1	D			S							X									230301	4.670.000	747.200	0	0	0	0	[illegible]	4.670.000	[illegible]	14-7	4.670.000	3	113.800	CCF22	4.670.000	186.800	4.670.000	0	0	0	0
92	CC	11366770	QUINTERO C[illegible] ALEXANDER	1	D			S																231001	6.000.000	960.000	0	0	30.000	30.000	[illegible]	[illegible]	[illegible]	14-7	6.000.000	3	146.200	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
93	CC	80035699	RODRIGUEZ[illegible] ARO FABIAN	1	D			S																25-14	2.300.000	368.000	0	0	0	0	[illegible]	[illegible]	[illegible]	14-7	2.300.000	3	56.100	CCF22	2.300.000	92.000	2.300.000	0	0	0	0
94	CC	1033887102	TOLOSA RIV[illegible] ER ANDRES	1	D			S							X									230301	2.045.455	327.300	0	0	0	0	EPS002	2.045.455	81.900	14-7	2.045.455	3	45.900	CCF22	2.045.455	81.900	2.045.455	0	0	0	0
95	CC	1016030560	CORDONADO L[illegible] ERSON SMITH	1	D			S								X								230301	1.423.500	227.800	0	0	0	0	EPS005	1.423.500	57.000	14-7	1.423.500	3	0	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
96	CC	1119893587	RODRIGUEZ BE[illegible] JOHNSON ANDRES	1	D			S							X									230301	3.527.727	564.500	0	0	0	0	EPS002	3.527.727	141.200	14-7	3.527.727	3	88.800	CCF22	3.527.727	141.200	3.527.727	0	0	0	0
97	CC	1070624193	CANDIA ORTE[illegible] JHON ANDRES	1	D			S							X									230301	2.770.908	443.400	0	0	0	0	EPS002	2.770.908	110.900	14-7	2.770.908	3	67.900	CCF22	2.770.908	110.900	2.770.908	0	0	0	0
98	CC	80869173	CAMPOS GALINDO JEISON JAIR	1	D			S	X						X									230301	430.303	68.900	0	0	0	0	EPS005	430.303	17.300	14-7	430.303	3	10.500	CCF22	1.154.860	46.200	1.154.860	0	0	0	0
99	CC	1075248955	PASCUAS ANDRADE JEISSON FERNANDO	1	D			S																230301	2.416.667	386.700	0	0	0	0	EPS037	2.416.667	96.700	14-7	2.416.667	3	59.900	CCF22	2.416.667	96.700	2.416.667	0	0	0	0
100	CC	1075248955	PASCUAS ANDRADE JEISSON FERNANDO	1	D			S											L					230301	83.333	13.400	0	0	0	0	EPS037	83.333	3.400	14-7	83.333	3	0	CCF22	83.333	3.400	83.333	0	0	0	0
101	CC	1033778192	OSORIO AMESQUITA JEISSON	1	D			S							X									231001	1.766.182	282.600	0	0	0	0	EPS017	1.766.182	70.700	14-7	1.766.182	3	43.100	CCF22	1.766.182	70.700	1.766.182	0	0	0	0
102	CC	79523643	ROJAS ESTUPIÑAN JEISSON	1	D			S							X									230301	1.827.636	308.500	0	0	0	0	EPS008	1.927.636	77.200	14-7	1.927.636	3	47.000	CCF22	1.927.636	77.200	1.927.636	0	0	0	0
103	CC	53153352	CAICEDO JENNIFER ASTRID	1	D			N							X									230301	12.953.850	2.072.700	0	0	64.800	64.800	EPS005	12.953.850	1.619.300	14-7	12.953.850	3	315.600	CCF22	12.953.850	518.200	12.953.850	259.100	388.700	0	0
104	CC	1022408442	CHACON TORRES JESSICA TATIANA	1	D			S							X									230301	3.156.363	505.100	0	0	0	0	EPS010	3.156.363	126.300	14-7	3.156.363	3	76.900	CCF22	3.156.363	126.300	3.156.363	0	0	0	0
105	CC	109388051	PUENAYAN QUICENO JESUS ALBERTO	1	D			S							X									230301	2.514.480	402.400	0	0	0	0	EPS008	2.514.480	100.600	14-7	2.514.480	3	61.300	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
106	CC	80544134	VARGAS ALONSO JESUS ALBERTO	1	D			S							X									230201	2.868.666	459.000	0	0	0	0	EPS037	2.868.666	114.800	14-7	2.868.666	3	69.900	CCF22	2.868.666	114.800	2.868.666	0	0	0	0
107	CC	52831059	TABARES [illegible]LEZ JEYMMY JOHANNA	1	D			S							X									230201	4.068.666	651.000	0	0	0	0	EPS008	4.068.666	162.800	14-7	4.068.666	3	99.200	CCF22	4.068.666	162.800	4.068.666	0	0	0	0
108	CC	1013652223	CARDENAS HERRERA JHOAN SEBASTIAN	1	D			S	X						X									230201	801.999	128.400	0	0	0	0	EPS001	801.999	32.100	14-7	801.999	3	16.600	CCF22	2.218.003	88.800	2.218.003	0	0	0	0
109	CC	1000974498	GALLEGO RIOS JHOJAN ESTIBEN	1	D			S	X						X									230301	454.667	72.800	0	0	0	0	EPS005	454.667	18.200	14-7	454.667	3	11.100	CCF22	1.404.561	56.200	1.404.561	0	0	0	0
110	CC	86062274	CABEZAS PISCO JHON ALEXANDER	1	D			S							X									230201	3.672.501	587.700	0	0	0	0	EPS005	3.672.501	147.000	14-7	3.672.501	3	89.500	CCF34	3.672.501	147.000	3.672.501	0	0	0	0
111	CC	1052393575	GARCIA ALBARRACIN JHONATAN ANDRES	1	D			S																230301	6.000.000	960.000	0	0	30.000	30.000	EPS017	6.000.000	240.000	14-7	6.000.000	3	146.200	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
112	CC	1000125892	LOPEZ TORRES JHONATAN DAVID	1	D			S													X	X		230301	2.068.666	331.000	0	0	0	0	EPS008	2.068.666	82.800	14-7	2.068.666	3	50.400	CCF22	2.068.666	82.800	2.068.666	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					185	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE								INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES					
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Cotiza Exterior	Exonerado	ING	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario o Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC	1124275**	HINESTROZA RENTERÍA JHONDEIBER	1	0			S																	25-14	1.423.500	227.800	0	0	0	0	NINGU	1.423.500	57.900	14-7	1.423.500	3	34.700	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
2	CC	100****285683	GARATEJO GARZON JOHAN SEBASTIAN	1	0			S								X									230301	1.133.818	181.500	0	0	0	0	EPS005	1.133.818	45.400	14-7	1.133.818	3	27.700	CCF22	1.133.818	45.400	1.133.818	0	0	0	0
3	CC	100****285683	GARATEJO GARZON JOHAN SEBASTIAN	1	0			S												X					230301	988.182	158.200	0	0	0	0	EPS005	988.182	39.600	14-7	988.182	3	0	CCF22	876.345	35.100	876.345	0	0	0	0
4	CC	1059768290	TORRES RIVERA JOHAN STIVEN	1	0			S								X									230901	2.247.272	359.600	0	0	0	0	EPS017	2.247.272	89.900	14-7	2.247.272	3	64.800	CCF22	2.247.272	89.900	2.247.272	0	0	0	0
5	CC	1022927571	BELLO GUITARRERO JOHN ALEXANDER	1	0			S								X									230201	3.092.046	494.800	0	0	0	0	EPS010	3.092.046	123.700	14-7	3.092.046	3	75.500	CCF22	3.092.046	123.700	3.092.046	0	0	0	0
6	CC	7548603**	CELIS NOVA JOHAN FREDY	1	0			N																	25-14	12.953.850	2.072.700	0	0	64.600	64.600	EPS0**	12.953.850	518.300	14-7	12.953.850	3	315.600	CCF22	12.953.850	518.200	12.953.850	259.100	388.700	0	0
7	CC	100****82565	COGUA LEAL JOHAN ESTEBAN	1	0			S																	25-14	4.500.000	720.000	0	0	0	0	EPS0**	4.500.000	180.000	14-7	4.500.000	3	109.700	CCF22	4.500.000	180.000	4.500.000	0	0	0	0
8	CC	1022388535	HONSHICA MACHADO JONATAN STEVEN	1	0			S																	25-14	5.068.666	811.000	0	0	0	0	EPS0**	5.068.666	202.800	14-7	5.068.666	3	123.500	CCF22	5.068.666	202.800	5.068.666	0	0	0	0
9	CC	1075624601	LOPEZ GAMEZ JOSE ALEJANDRO	1	0			S																	230201	1.800.000	288.000	0	0	0	0	EPS005	1.800.000	72.000	14-7	1.800.000	3	43.900	CCF22	1.800.000	72.000	1.800.000	0	0	0	0
10	CC	1075624601	LOPEZ GAMEZ JOSE ALEJANDRO	1	0			S																	230701	136.162	21.800	0	0	0	0	EPS005	136.162	5.400	14-7	136.162	3	0	CCF22	136.162	5.400	136.162	0	0	0	0
11	CC	1075624601	LOPEZ GAMEZ JOSE ALEJANDRO	1	0			S																	230201	86.667	13.900	0	0	0	0	EPS005	66.667	2.700	14-7	66.667	3	0	CCF22	69.867	2.800	69.867	0	0	0	0
12	CC	1076294897	RAMIREZ SOLANO JORGE EDUARDO	1	0			S								X									230301	5.122.344	819.600	0	0	25.700	25.700	EPS008	5.122.344	204.900	14-7	5.122.344	3	124.600	CCF22	5.122.344	204.900	5.122.344	0	0	0	0
13	CC	1076294897	RAMIREZ SOLANO JORGE EDUARDO	1	0			S												X					230301	646.156	103.300	0	0	6.500	6.500	EPS008	646.156	25.900	14-7	646.156	3	0	CCF22	637.617	25.600	637.617	0	0	0	0
14	CC	1026630680	ROJAS VILLAMIL JORGE HERNANDO	1	0			S								X									230201	2.819.347	451.100	0	0	0	0	EPS005	2.819.347	112.800	14-7	2.819.347	3	68.700	CCF22	2.819.347	112.800	2.819.347	0	0	0	0
15	CC	94153133	PRIETO MUÑOZ JOSE ANTONIO	1	0			N																	25-14	1.376.050	220.200	0	0	0	0	MINI01	1.376.050	172.100	14-7	1.376.050	3	33.600	CCF22	13.761	600	13.761	300	500	0	0
16	CC	94153133	PRIETO MUÑOZ JOSE ANTONIO	1	0			N															L		25-14	47.450	7.600	0	0	0	0	MINI01	47.450	6.000	14-7	47.450	3	0	CCF22	47.450	1.900	47.450	1.000	1.500	0	0
17	CC	80246551	VIRVIESCAS SOTELO JOSE MIGUEL	1	0			S																	230301	1.933.334	309.400	0	0	0	0	EPS009	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
18	CC	80246551	VIRVIESCAS SOTELO JOSE MIGUEL	1	0			S												X					230301	75.504	12.100	0	0	0	0	EPS008	75.504	3.100	14-7	75.504	3	0	CCF22	75.504	3.100	75.504	0	0	0	0
19	CC	1070588915	GUEVARA MEDINA JOSE YESID	1	0			S																	230901	4.500.000	720.000	0	0	0	0	EPS005	4.500.000	180.000	14-7	4.500.000	3	109.700	CCF22	4.500.000	180.000	4.500.000	0	0	0	0
20	CC	1026560301	MENDOZA MUÑOZ JOSSARY DEL CARMEN	1	0			S																	25-14	1.423.500	227.800	0	0	0	0	EPS008	1.423.500	57.000	14-7	1.423.500	3	34.700	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
21	CC	1067380811	LUCERO PEREZ JUAN ANDRES	1	0			S								X									230301	2.116.364	338.700	0	0	0	0	EPS037	2.116.364	84.700	14-7	2.116.364	3	51.600	CCF22	2.116.364	84.700	2.116.364	0	0	0	0
22	CC	1027150193	CASTRO RUIZ JUAN CAMILO	1	0			S								X									230301	1.774.268	283.900	0	0	0	0	EPS005	1.774.268	71.000	14-7	1.774.268	3	43.300	CCF22	1.774.268	71.000	1.774.268	0	0	0	0
23	CC	80373815	ORTIZ RODRIGUEZ JUAN CAMILO	1	0			S								X									230301	2.360.727	377.800	0	0	0	0	EPS005	2.360.727	94.500	14-7	2.360.727	3	57.600	CCF22	2.360.727	94.500	2.360.727	0	0	0	0
24	CC	1014202564	SALAZAR GIL JUAN CAMILO	1	0			S								X									25-14	3.602.332	576.400	0	0	0	0	EPS017	3.602.332	144.100	14-7	3.602.332	3	87.800	CCF22	3.602.332	144.100	3.602.332	0	0	0	0
25	CC	1012448443	ARREGOCES CUERO JUAN CARLOS	1	0			S								X									230301	3.852.188	616.400	0	0	0	0	EPS008	3.852.188	154.100	14-7	3.852.188	3	93.900	CCF22	3.852.188	154.100	3.852.188	0	0	0	0
26	CC	1012448443	ARREGOCES CUERO JUAN CARLOS	1	0			S												X					230301	282.894	45.300	0	0	0	0	EPS008	282.894	11.400	14-7	282.894	3	0	CCF22	244.379	9.800	244.379	0	0	0	0
27	CC	1012457670	VEGA VELANDIA JUAN CARLOS	1	0			S	X							X									230201	892.121	110.800	0	0	0	0	EPSC34	892.121	27.700	14-7	892.121	3	16.900	CCF22	1.666.734	66.700	1.666.734	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
PERIODO SALUD	PERIODO PENSIONES				185	0
					TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Colegio	Aprendiz	Extranjero	Cotiz. a fondo de solidaridad	Exonerado	IRP	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	COMENTARIOS	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
40	CC	1032476481	BELLO GARAY JUAN DAVID	1	0			S								X								230201	2.656.819	425.100	0	0	0	0	EPS002	2.656.819	106.300	14-7	2.656.819	3	64.800	CCF22	2.656.819	106.300	2.656.819	0	0	0	0
41	TI	1031651014	BERMUDEZ MUÑOZ JUAN DAVID	1	0			S								X								25-14	1.658.113	265.300	0	0	0	0	EPS037	1.658.113	66.400	14-7	1.658.113	3	40.400	CCF22	1.658.113	66.400	1.658.113	0	0	0	0
42	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S								X								230201	1.633.254	261.400	0	0	0	0	EPS010	1.633.254	65.400	14-7	1.633.254	3	39.600	CCF22	1.633.254	65.400	1.633.254	0	0	0	0
43	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S								X								230201	69.123	11.100	0	0	0	0	EPS010	69.123	2.800	14-7	69.123	3	0	CCF22	69.123	2.800	69.123	0	0	0	0
44	CC	1031641672	ROJAS TIQUE JUAN DAVID	1	0			S								X								230201	138.245	22.200	0	0	0	0	EPS010	138.245	5.600	14-7	138.245	3	0	CCF22	138.245	5.600	138.245	0	0	0	0
45	CC	80*98836	YARA TO JUAN DAVID	1	0			S								X								25-14	3.170.455	507.300	0	0	0	0	EPS037	3.170.455	126.900	14-7	3.170.455	3	77.300	CCF22	3.170.455	126.900	3.170.455	0	0	0	0
46	CC	1000513272	ZAPATA MA JUAN DIEGO	1				S								X								230301	1.933.334	309.400	0	0	0	0	EPS	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
47	CC	1000513272	ZAPATA MA JUAN DIEGO	1				S								L								230301	66.667	10.700	0	0	0	0		66.667		14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
48	CC	1070987313	ORTIZ SIMBAC	1	0			S								X								231001	1.761.382	281.900	0	0	0	0		1.761.382		14-7	1.761.382	3	43.000	CCF22	1.761.382	70.400	1.761.382	0	0	0	0
49	CC	1005068478	SEPULVEDA ZAR KEINNY	1	0			S	X															230201	2.500.000	400.000	0	0	0	0		2.500.000		14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
50	CC	1031178108	PEREZ CARD YN ANDRES	1	0			S								X								230201	2.202.906	352.500	0	0	0	0	EPS037	2.202.906	88.200	14-7	2.202.906	3	53.700	CCF22	2.202.906	88.200	2.202.906	0	0	0	0
51	CC	1022976568	QUISOBONY KEVIN JULIAN	1	0			S	X							X								230201	484.667	77.500	0	0	0	0	EPS005	484.667	19.400	14-7	484.667	3	12.100	CCF22	2.284.667	91.700	2.284.667	0	0	0	0
52	CC	1076667875	PAEZ GOMEZ LAURA YURANI	1	0			S								X								230201	5.000.000	800.000	0	0	0	0	EPS017	5.000.000	200.000	14-7	5.000.000	3	121.900	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
53	CC	1033593589	PINZON DUARTE FEIDY LORENA	1	0			S																25-14	3.000.000	480.000	0	0	0	0	EPS017	3.000.000	120.000	14-7	3.000.000	3	73.100	CCF22	3.000.000	120.000	3.000.000	0	0	0	0
54	CC	1031158359	GARZON TIRANO LEONARDO DAVID	1	0			S								X								230301	1.917.819	306.900	0	0	0	0	EPS005	1.917.819	76.800	14-7	1.917.819	3	46.800	CCF22	1.917.819	76.800	1.917.819	0	0	0	0
55	CC	79717994	GONZALEZ HERRERA LEONARDO	1	0			S																25-14	2.000.000	320.000	0	0	0	0	EPS005	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
56	CC	1110294851	TORRES VERBEL LISETH ROCIO	1	0			S																231001	1.525.000	244.000	0	0	0	0	EPS002	1.525.000	61.000	14-7	1.525.000	3	37.200	CCF22	1.525.000	61.000	1.525.000	0	0	0	0
57	CC	52691378	SCARPETTA MANCHA LITZA MARIA	1	0			S																230201	1.800.000	288.000	0	0	0	0	EPS017	1.800.000	72.000	14-7	1.800.000	3	43.900	CCF22	1.800.000	72.000	1.800.000	0	0	0	0
58	CC	1090452479	SARRIS ROZO LIZETH CAROLINA	1	0			S																230301	2.500.000	400.000	0	0	0	0	EPS017	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
59	CC	1067728990	MANOUILLO LAGOS LUCERO MARISOL	1	0			S																230301	5.694.000	911.100	0	0	28.500	28.500	EPS005	5.694.000	227.800	14-7	5.694.000	3	138.800	CCF14	5.694.000	227.800	5.694.000	0	0	0	0
60	PT	1062643	OVALLES LAMONT LUIS RAFAEL	1	0			S								X								230301	1.879.928	300.800	0	0	0	0	EPS008	1.879.928	75.200	14-7	1.879.928	3	45.800	CCF22	1.879.928	75.200	1.879.928	0	0	0	0
61	CC	1022989169	RUGE ARJONA LUIS ALFREDO	1	0			S																230201	3.266.667	522.700	0	0	0	0	EPS002	3.266.667	130.700	14-7	3.266.667	3	79.600	CCF22	3.266.667	130.700	3.266.667	0	0	0	0
62	CC	1022989169	RUGE ARJONA LUIS ALFREDO	3	0			S								X								230201	241.715	38.700	0	0	0	0	EPS002	241.715	9.700	14-7	241.715	3	0	CCF22	241.715	9.700	241.715	0	0	0	0
63	CC	1067698775	MARTINEZ ACOSTA LUIS CARLOS	1	0			S					X											230301	9.500.000	1.520.000	0	0	47.500	47.500	EPS005	9.500.000	380.000	14-7	9.500.000	3	231.500	CCF22	9.500.000	380.000	9.500.000	0	0	0	0
64	CC	79215255	LOPEZ FELICIANO LUIS FERNANDO	1	0			S								X								25-14	2.275.000	364.000	0	0	0	0	EPS017	2.275.000	91.000	14-7	2.275.000	3	55.500	CCF22	2.275.000	91.000	2.275.000	0	0	0	0
65	CC	1007641013	PULIDO LA TORRE LUISA FERNANDA	1	0			S																25-14	2.500.000	400.000	0	0	0	0	EPS005	2.500.000	100.000	14-7	2.500.000	3	60.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
66	CC	40340479	TOTE PEÑA LUZ ADRIANA	1	0			S	X							X								230301	435.394	69.700	0	0	0	0	EPS008	435.394	17.500	14-7	435.394	3	10.700	CCF22	1.436.412	57.500	1.436.412	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO
NI	900311748-1	YEAPDATA SAS		Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	EXONERADO PAGO PARAFISCALES Y SALUD
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ, D. C.	BOGOTA, D.C.	SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD
					EMPLEADOS: 185 / UPC: 0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE								INFORMACIÓN NOVEDADES																				PENSIÓN							SALUD			RIESGOS LABORALES				CCF				PARAFISCALES					
No.	Tipo	No. de Identificación	Apellidos y Nombres	Colegiado	Salario	Extranjero	Cotiz. Exterior	Sustitución	ING	RET	TDE	TAE	TDP	TAP	SLN	IGE	LMA	VAC	AVP	VST	AL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC	1013640452	HERNANDEZ TORRIJOS LUZ KATHERINE	1	0			S							X								230201	2.288.000	366.100	0	0	0	0	EPS002	2.288.300	91.600	14-7	2.288.300	3	55.000	CCF22	2.288.000	91.600	2.288.000	0	0	0	0
2	CC	1000119237	ARDILA ALONSO MARCOL CAMILO	1	0			S							X								230301	1.827.746	292.500	0	0	0	0	EPS010	1.827.746	73.200	14-7	1.827.746	3	44.000	CCF22	1.827.746	73.200	1.827.746	0	0	0	0
3	CC	1019133315	ALVARADO CARRILLO MAIRA ALEJANDRA	1	0			S							X								230301	649.718	104.000	0	0	0	0	EPS001	649.718	26.000	14-7	649.718	3	15.900	CCF22	649.718	26.000	649.718	0	0	0	0
4	CC	1019133315	ALVARADO CARRILLO MAIRA ALEJANDRA	1	0			S								X							230301	121.457	19.500	0	0	0	0	EPS001	121.457	4.900	14-7	121.457	3	0	CCF22	121.457	4.900	121.457	0	0	0	0
5	CC	1019133315	ALVARADO CARRILLO MAIRA ALEJANDRA	1	0			S								X							230301	182.186	29.300	0	0	0	0	EPS001	182.186	7.300	14-7	182.186	3	0	CCF22	182.186	7.300	182.186	0	0	0	0
6	CC	1019133315	ALVARADO CARRILLO MAIRA ALEJANDRA	1	0			S								X							230301	910.931	146.500	0	0	0	0	EPS001	910.931	36.500	14-7	910.931	3	0	CCF22	910.931	36.500	910.931	0	0	0	0
7	CC	1015484383	ANGARITA PULIDO MARIA CLAUDIA	1	0			S															230201	2.000.000	320.000	0	0	0	0	EPS017	2.000.000	80.000	14-7	2.000.000	3	46.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
8	CC	1015461601	PINZON PINZON MARIA PAULA	1	0			S															230901	5.000.000	800.000	0	0	0	0	EPS008	5.000.000	200.000	14-7	5.000.000	3	121.800	CCF22	5.000.000	200.000	5.000.000	0	0	0	0
9	CC	1000686502	ORJUELA HERNANDEZ MARIA TATIANA	1	0			S															230301	1.866.667	298.700	0	0	0	0	EPS017	1.866.667	74.700	14-7	1.866.667	3	45.500	CCF22	1.866.667	74.700	1.866.667	0	0	0	0
10	CC	1000686507	ORJUELA HERNANDEZ MARIA TATIANA	1	0			S															230301	142.111	22.800	0	0	0	0	EPS017	142.111	5.700	14-7	142.111	3	0	CCF22	142.111	5.700	142.111	0	0	0	0
11	CC	79874518	RUAÑO PARRA MIGUEL ANGEL	1	0			S							X								230201	1.899.272	303.900	0	0	0	0	EPS017	1.899.272	76.000	14-7	1.899.272	3	46.900	CCF22	1.899.272	76.000	1.899.272	0	0	0	0
12	CC	80470478	VIVEROS CORREDOR MIGUEL GONZALO	1	0			S															25-14	1.333.334	213.400	0	0	0	0	EPS005	1.333.334	53.400	14-7	1.333.334	3	32.500	CCF22	1.333.334	53.400	1.333.334	0	0	0	0
13	CC	80470478	VIVEROS CORREDOR MIGUEL GONZALO	1	0			S												X			25-14	711.212	113.800	0	0	0	0	EPS005	711.212	28.500	14-7	711.212	3	0	CCF22	684.212	27.400	684.212	0	0	0	0
14	CC	79896895	BERNAL CASTILLO NELSON ALEXANDER	1	0			S															230201	6.000.000	960.000	0	0	30.000	30.000	EPS008	6.000.000	240.000	14-7	6.000.000	3	146.700	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
15	CC	80783173	ROCHA SEGURA NESTOR ALFREDO	1	0			S							X								230301	4.602.272	736.400	0	0	0	0	EPS008	4.602.272	184.100	14-7	4.602.272	3	112.200	CCF22	4.602.272	184.100	4.602.272	0	0	0	0
16	CC	1192762659	MATALLANA ROCHA NICOLAS SEBASTIAN	1	0			S							X								230301	2.581.999	413.200	0	0	0	0	EPS005	2.581.999	103.300	14-7	2.581.999	3	62.900	CCF22	2.581.999	103.300	2.581.999	0	0	0	0
17	CC	1192762659	MATALLANA ROCHA NICOLAS SEBASTIAN	1	0			S											L				230301	86.667	13.900	0	0	0	0	EPS005	86.667	3.500	14-7	86.667	3	0	CCF22	86.667	3.500	86.667	0	0	0	0
18	CC	1014196425	NEIRA ANGULO NINI JOHANNA	1	0			S															230201	3.500.000	560.000	0	0	0	0	EPS005	3.500.000	140.000	14-7	3.500.000	3	85.300	CCF22	3.500.000	140.000	3.500.000	0	0	0	0
19	CC	1001845178	MANOSALVA SANCHEZ OMAR LEONARDO	1	0			S							X								230301	2.057.455	329.200	0	0	0	0	EPS017	2.057.455	82.300	14-7	2.057.455	3	50.200	CCF22	2.260.830	90.500	2.260.830	0	0	0	0
20	CC	1012386535	LOPEZ CASANOVA OSCAR ALEXANDER	1	0			S															230301	1.980.000	316.800	0	0	0	0	EPS002	1.980.000	79.200	14-7	1.980.000	3	48.300	CCF22	1.980.000	79.200	1.980.000	0	0	0	0
21	CC	91287244	CONTRERAS FERNANDEZ OSCAR ANDRES	1	0			S															25-14	8.000.000	1.280.000	0	0	40.000	40.000	EPS005	8.000.000	320.000	14-7	8.000.000	3	194.900	CCF22	8.000.000	320.000	8.000.000	0	0	0	0
22	CC	1115183788	VELEZ ORREGO OSCAR ENRIQUE	1	0			S	X														230301	10.800.000	1.728.000	0	0	54.000	54.000	EPS017	10.800.000	432.000	14-7	10.800.000	3	263.100	CCF22	10.800.000	432.000	10.800.000	0	0	0	0
23	CC	1030623331	BARBOSA GONZALEZ OSCAR HERNAN	1	0			S							X								230301	7.763.636	1.242.200	0	0	38.900	38.900	EPS017	7.763.636	310.900	14-7	7.763.636	3	189.200	CCF22	7.763.636	310.900	7.763.636	0	0	0	0
24	CC	1072643037	CALDERON MARIN OSCAR IVAN	1	0			S															25-14	3.866.667	618.700	0	0	0	0	EPS010	3.866.667	154.700	14-7	3.866.667	3	94.200	CCF22	3.866.667	154.700	3.866.667	0	0	0	0
25	CC	1072643037	CALDERON MARIN OSCAR IVAN	1	0			S												X			25-14	126.923	20.400	0	0	0	0	EPS010	126.923	5.100	14-7	126.923	3	0	CCF22	126.923	5.100	126.923	0	0	0	0
26	CC	86057522	RIVEROS TORRES OSCAR IVAN	1	0			S							X								25-14	3.105.227	496.900	0	0	0	0	EPS005	3.105.227	124.300	14-7	3.105.227	3	75.700	CCF34	3.105.227	124.300	3.105.227	0	0	0	0
27	CC	80251420	SICHACA DIAZ OSCAR IVAN	1	0			S							X								230201	5.137.332	822.000	0	0	0	0	EPS008	5.137.332	205.500	14-7	5.137.332	3	175.200	CCF22	5.137.332	205.500	5.137.332	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 cot	YEAPDATA	YEAPDATA	BOGOTÁ, D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					185	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																	PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Colombiano en el Exterior	Residente	IGE	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario o Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase o Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
14	CC	1019100559	VILLAFAÑE PORRAS PATRICIA ISABEL	1	0			S						X										230901	6.068.666	971.000	0	0	30.400	30.400	EPS008	6.068.666	242.800	14-7	6.068.666	3	147.900	CCF22	6.068.666	242.800	6.068.666	0	0	0	0
15	CC	1044391335	CORONEL RODRIGUEZ PEDRO ALEXANDER	1	0			S						X										230201	3.491.394	558.700	0	0	0	0	EPS005	3.491.394	139.700	14-7	3.491.394	3	85.100	CCF22	3.491.394	139.700	3.491.394	0	0	0	0
16	CC	1012437605	MARTINEZ ROMERO RAFAEL STEVEN	1	0			S						X										230301	5.041.395	806.700	0	0	0	0	EPS008	5.041.395	201.700	14-7	5.041.395	3	122.900	CCF22	5.041.395	201.700	5.041.395	0	0	0	0
17	CC	1020622956	LEON LEON PAUL EDUARDO	1	0			S						X										231001	2.836.364	453.900	0	0	0	0	EPS005	2.836.364	113.500	14-7	2.836.364	3	69.100	CCF22	2.836.364	113.500	2.836.364	0	0	0	0
18	CC	1073704285	GUIO [illegible]ARDO	1	0			S						X										230301	2.205.606	352.900	0	0	0	0	EPS008	2.205.606	88.300	14-7	2.205.606	3	53.800	CCF22	2.205.606	88.300	2.205.606	0	0	0	0
19	CC	1073704285	GUIO [illegible]ARDO	1	0			S						X										230301	72.189	11.600	0	0	0	0	EPS008	72.189	2.900	14-7	72.189	3	0	CCF22	72.189	2.900	72.189	0	0	0	0
20	CC	1077468930	RENTERIA [illegible]A ROIDER	1	0			S						X										230301	1.923.636	307.600	0	0	0	0	EPS008	1.923.636	77.000	14-7	1.923.636	3	46.900	CCF22	1.923.636	77.000	1.923.636	0	0	0	0
21	CC	1030661109	CARVAJAL CALD[illegible]ONAL EDUARDO	1	0			S						X										230901	3.150.000	504.000	0	0	0	0	EPS005	3.150.000	126.000	14-7	3.150.000	3	76.900	CCF22	3.150.000	126.000	3.150.000	0	0	0	0
22	CC	25882805	CORREA [illegible]ORA LINA	1	0			S						X										25-14	5.500.000	880.000	0	0	0	0	EPS005	5.500.000	220.000	14-7	5.500.000	3	134.000	CCF22	5.500.000	220.000	5.500.000	0	0	0	0
23	CC	1012385381	ROJAS R[illegible]EN DARIO	1	0			S						X										230301	2.558.400	409.400	0	0	0	0	EPS008	2.558.400	102.400	14-7	2.558.400	3	62.400	CCF22	2.558.400	102.400	2.558.400	0	0	0	0
24	CC	1012385381	ROJAS R[illegible]EN DARIO	1	0			S						X										230301	60.000	9.600	0	0	0	0	EPS002	60.000	2.400	14-7	60.000	3	0	CCF22	60.000	2.400	60.000	0	0	0	0
25	CC	1021156423	GOMEZ FI[illegible]NO SAMIR YECID	1	0			S						X										230301	6.266.868	1.002.700	0	0	39.400	39.400	EPS005	6.266.868	250.800	14-7	6.266.868	3	157.800	CCF22	6.266.868	250.800	6.266.868	0	0	0	0
26	CC	1006606096	GALINDO [illegible]CHIMA SAMUEL	1	0			S																230301	1.423.500	227.800	0	0	0	0	MIN001	1.423.500	57.000	14-7	1.423.500	3	34.700	CCF22	1.423.500	57.000	1.423.500	0	0	0	0
27	CC	1027402973	NIÑO URIBE SANTIAGO	1	0			S						X										230301	2.345.454	375.300	0	0	0	0	EPS008	2.345.454	93.900	14-7	2.345.454	3	57.200	CCF22	2.345.454	93.900	2.345.454	0	0	0	0
28	CC	1026256577	MORALES GALINDO SEBASTIAN	1	0			S						X										230201	6.068.666	971.000	0	0	30.400	30.400	EPS005	6.068.666	242.800	14-7	6.068.666	3	147.900	CCF22	6.068.666	242.800	6.068.666	0	0	0	0
29	CC	1022371537	ROBERTO RODRIGUEZ SEBASTIAN	1	0			S						X										231001	4.610.164	737.700	0	0	0	0	EPS005	4.610.164	184.500	14-7	4.610.164	3	112.400	CCF22	4.583.334	183.400	4.583.334	0	0	0	0
30	CC	1022371537	ROBERTO RODRIGUEZ SEBASTIAN	1	0			S												X				231001	938.889	150.300	0	0	0	0	EPS005	938.889	37.600	14-7	938.889	3	0	CCF22	885.790	35.500	885.790	0	0	0	0
31	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S						X										231001	2.137.335	342.000	0	0	0	0	EPS005	2.137.335	85.500	14-7	2.137.335	3	52.100	CCF22	2.137.335	85.500	2.137.335	0	0	0	0
32	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S						X										231001	466.667	74.700	0	0	0	0	EPS005	466.667	0	14-7	466.667	3	0	CCF22	466.667	0	466.667	0	0	0	0
33	CC	1016019176	BAEZ PAEZ SERGIO ANDRES	1	0			S												X				231001	66.667	10.700	0	0	0	0	EPS005	66.667	2.700	14-7	66.667	3	0	CCF22	66.667	2.700	66.667	0	0	0	0
34	CC	80876276	RAMIREZ ORTIZ SERGIO IVAN	1	0			S						X										230901	7.137.332	1.142.000	0	0	35.700	35.700	EPS017	7.137.332	285.500	14-7	7.137.332	3	179.900	CCF22	7.137.332	285.500	7.137.332	0	0	0	0
35	CC	1018618106	OROZCO PEREZ SINDY PAOLA	1	0			S						X										25-14	3.080.000	492.800	0	0	0	0	EPS010	3.080.000	123.200	14-7	3.080.000	3	75.100	CCF22	3.080.000	123.200	3.080.000	0	0	0	0
36	CC	1000123544	ANGARITA CASTELLANOS TATIANA ANDREA	1	0			S						X										230301	951.382	152.300	0	0	0	0	EPS010	951.382	38.100	14-7	951.382	3	23.200	CCF22	951.382	38.100	951.382	0	0	0	0
37	CC	1000123544	ANGARITA CASTELLANOS TATIANA ANDREA	1	0			S												X				230301	866.332	138.700	0	0	0	0	EPS010	866.332	34.700	14-7	866.332	3	0	CCF22	831.294	33.300	831.294	0	0	0	0
38	CC	1000491684	VALENCIA MUÑOZ TATIANA	1	0			S																25-14	2.000.000	320.000	0	0	0	0	EPS002	2.000.000	80.000	14-7	2.000.000	3	46.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0
39	CC	1072322232	PARRA PADILLA THOMAS ALEJANDRO	1	0			S						X										230301	2.121.955	339.600	0	0	0	0	EPS002	2.121.955	84.900	14-7	2.121.955	3	51.700	CCF22	2.121.955	84.900	2.121.955	0	0	0	0
40	CC	1022444863	BOLIVAR ARAQUE VALENTINA	1	0			S																230301	2.000.000	320.000	0	0	0	0	EPS008	2.000.000	80.000	14-7	2.000.000	3	48.800	CCF22	2.000.000	80.000	2.000.000	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900311748-1	YEAPDATA SAS	Carrera 19B # 84-17 Ofc 403- 404	3154028330	compliance@yeapdata.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	A – Más de 200 col	YEAPDATA	YEAPDATA	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					185	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	05/12/2025	92119873	$182.898.300	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																PENSIÓN						SALUD			RIESGOS LABORALES			CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Cotiza Custodia	Pensionado	IGE	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cod. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
22 1	CC	1013198563	QUECAN AGUDELO AHILEMAR ALEJANDRO	1	0			S								X								230201	3.068.666	491.000	0	0	0	0	EPS005	3.068.666	122.800	14-7	3.068.666	3	74.900	CCF22	3.068.666	122.800	3.068.666	0	0	0	0
22 2	CC	1000063900	BLANCO LIZARAZO WILLIAM DAVID	1	0			S																230201	2.500.000	400.000	0	0	0	0	EPS017	2.500.000	100.000	14-7	2.500.000	3	50.900	CCF22	2.500.000	100.000	2.500.000	0	0	0	0
22 3	CC	1073166085	CARDONA DIAZ WILMER STIVEN	1	0			S																230301	1.933.334	309.400	0	0	0	0	EPS017	1.933.334	77.400	14-7	1.933.334	3	47.100	CCF22	1.933.334	77.400	1.933.334	0	0	0	0
22 4	CC	1073166085	CARDONA DIAZ WILMER STIVEN	1	0			S																230301	66.667	10.700	0	0	0	0	EPS017	66.667	2.700	14-7	66.667	0	0	CCF22	66.667	2.700	66.667	0	0	0	0
22 5	CC	1032411578	MARIN CASTILLO WILSON FERNEY	1	0			S																25-14	3.000.000	480.000	0	0	0	0	EPS017	3.000.000	120.000	14-7	3.000.000	3	73.100	CCF22	3.000.000	120.000	3.000.000	0	0	0	0
22 6	CC	1070074461	GOMEZ QUINTERO [illegible]MARA VANESSA	1	0			S	X															25-14	2.660.000	425.600	0	0	0	0	EPS005	2.660.000	106.400	14-7	2.660.000	3	64.900	CCF22	2.660.000	106.400	2.660.000	0	0	0	0
22 7	CC	1069758230	GALEANO [illegible] JUAN CARLOS	1	0			S	X															230101	355.787	57.000	0	0	0	0	EPS005	355.787	14.300	14-7	355.787	3	8.700	CCF14	631.872	25.000	631.877	0	0	0	0
22 8	CC	1024549248	MALAMBO QUIVEN [illegible] JENNER NICOLAS	1	0			S																230301	1.932.000	309.200	0	0	0	0	EPS005	1.932.000	77.300	14-7	1.932.000	3	47.100	CCF22	1.932.000	77.300	1.932.000	0	0	0	0
22 9	CC	1070982509	ARIAS CASTILLO [illegible] ANTHONNE	1	0			S																230301	1.423.000	227.800	0	0	0	0	EPS005	1.423.500	56.900	14-7	1.423.500	3	34.700	CCF22	711.750	28.500	711.750	0	0	0	0
23 0	CC	1030610278	RODRIGUEZ RO [illegible] URY MARCELA	1	0			S																25-14	6.000.000	960.000	0	0	30.000	30.000	EPS005	6.000.000	240.000	14-7	6.000.000	3	146.200	CCF22	6.000.000	240.000	6.000.000	0	0	0	0
23 1	CC	1075682863	ROMERO [illegible] ALEIBY	1	0			S																230301	3.000.000	480.000	0	0	0	0	EPS017	3.000.000	120.000	14-7	3.000.000	3	73.100	CCF22	3.000.000	120.000	3.000.000	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

GEDESPROS.A.S
NIT: 900695249 - 3

BOKS INTERNATIONAL

EL SUSCRITO REVISOR FISCAL DE
YEAPDATA SAS
NIT 900.311.748-1

CERT-056 09-12-2025 - YEAP

CERTIFICA QUE:

YEAPDATA SAS identificada con **NIT No. 900.311.748-1** (En adelante la Compañía), efectuó los aportes parafiscales (SENA, ICBF y Cajas de Compensación Familiar), seguridad social (Pensión y ARL) correspondiente al mes de **noviembre** del Dos Mil Veinticinco (2025), y de salud del mes de **diciembre** del Dos Mil Veinticinco (2025), según la planillas **No. 92124350** y **92119873** liquidada y pagada a través del operador de información "Aportes en Línea" las cuales fueron canceladas el Cinco (05) de diciembre del Dos Mil Veinticinco (2025).

La Compañía ha dado cumplimiento a los dispuesto en la **Ley 100 De 1993, Ley 789 De 2002 (Art 50), Ley 797 De 2003; Decreto 1703 De 2002, Decreto 2170 De 2002** y demás normas vigentes relacionadas con el pago de obligaciones de Sistema de Seguridad Social Integral y Aportes Parafiscales.

A la fecha de expedición de la presente, la Compañía se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral y lo que corresponde a Aportes Parafiscales de los Once (11) meses anteriores a esta certificación

Se expide la presente certificación en la ciudad de Bogotá a los Nueve (09) días de diciembre del año Dos Mil Veinticinco (2025), a solicitud de la administración de la Compañía.

Cordialmente,

FRANKLIN E. BARRERA CASTAÑEDA
Revisor Fiscal
Tarjeta Profesional No. 172038-T
Designado por **GEDESPRO S.A.S.**
Tarjeta de Registro No. 1787

AK 45 #122-56 / Ofi. 709
Edificio Argenta - Bogotá D.C

(601) 9260160 - 301 4764654

administrativoRRHH@gedespro.com.co

www.gedespro.com.co

THE WINNER

Heimcore

CERTIFICACIÓN DE CUMPLIMIENTO ARTICULO 50 LEY 798 DE 2002 Y LEY 828 DE 2003

PERSONA JURIDICA

Yo, **DIANA MARIA MENDEZ GARNICA** identificado con cédula de ciudadanía No. **39.804.649**, de Cajica y con Tarjeta Profesional No.193872-T de la Junta Central de Contadores de Colombia, en mi condición de **REVISOR FISCAL** de **HEIMCORE SAS**, identificada con Nit. **900.425.697-2** debidamente inscrito ante la Cámara de Comercio de Bogotá, luego de examinar de acuerdo con las normas de auditoria generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico el pago de los aportes de seguridad social (pensión, salud y riesgos laborales) y de los aportes parafiscales (Instituto Colombiano de Bienestar familiar ICBF, Servicio Nacional de Aprendizaje SENA y Caja de Compensación Familiar), Obligaciones laborales, salaries y prestaciones sociales, cuando a ello hubiere lugar pagados por la compañía durante los últimos seis (6) meses legalmente exigibles a la fecha de la emisión de esa certificación, dichos pagos corresponden a los montos contabilizados y cancelados por la compañía durante dichos 6 meses. Lo anterior, en cumplimiento de lo dispuesto en el articulo 50 de la Ley 789 de 2002.

Nota 1: Para certificar el pago de los aportes correspondientes a los Sistemas de Seguridad Social y en el caso del pago correspondiente a los aportes parafiscales, se deberán tener en cuenta los plazos previstos de Decreto 1670 de 2007.

Se expide en Bogotá D.C, al primero de diciembre de 2025.

DIANA MARIA MENDEZ GARNICA
REVISOR FISCAL
C.C. 39.804.649 de Cajica
T.P. 193872-T



INDICE DERECHO

FECHA DE NACIMIENTO 02-ENE-1985

BOGOTA D.C.
(CUNDINAMARCA)
LUGAR DE NACIMIENTO

1.58 ESTATURA | O+ G.S. RH | F SEXO

21-ENE-2003 CAJICA
FECHA Y LUGAR DE EXPEDICION

REGISTRADORA NACIONAL
ALMABEATRIZ RENGIFO LOPEZ

P-1503100-39118411-F-0039804649-20030827 04714 03238A 02 136593590

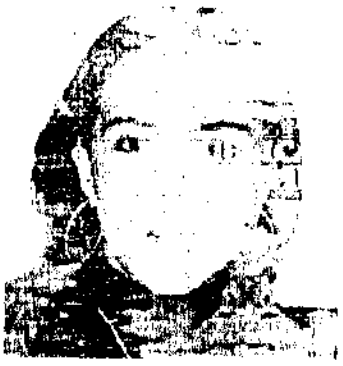
REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

NUMERO 39.804.649

MENDEZ GARNICA
APELLIDOS

DIANA MARIA
NOMBRES

FIRMA



República de Colombia
Ministerio de Comercio Industria y Turismo

JUNTA CENTRAL DE CONTADORES

TARJETA PROFESIONAL
DE CONTADOR PUBLICO

193872-T



DIANA MARIA
BENDEZ CANTE
C.C. 39804819

RESOLUCION INSCRIPCION 1217 FECHA 09/09/2014

UNIVERSIDAD

DIRECTOR GENERAL

JULIO CESAR ACUÑA GONZALEZ 203099

195208

Esta tarjeta es el unico documento que lo acredita como CONTADOR PUBLICO de acuerdo con lo establecido en la ley 43 de 1990.
Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: 644 44 50 o devolverla a la UAE - Junta Central de Contadores a la calle 96 No. 9A - 21 Bogota D.C.

www.ideas.com

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Certificado No:

LA REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

UNIDAD ADMINISTRATIVA ESPECIAL

JUNTA CENTRAL DE CONTADORES

CERTIFICA A:
QUIEN INTERESE

Que el contador público **DIANA MARIA MENDEZ GARNICA** identificado con CÉDULA DE CIUDADANÍA No 39804649 de CAJICA (CUNDINAMARCA) Y Tarjeta Profesional No 193872-T Sí tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de inscripción.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS * * *

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
CC 79906707		GODOY LOPEZ EDGAR ALFONSO	INDEPENDIENTE	PRINCIPAL	CRA QUINTA # 2- 35 MANZANA 21 CASA 208	MOSQUERA-CUNDINAMARCA	8272125	No

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2025-11	2025-11	2000405053	94950008625	I	2025/12/02	2025/12/11	BANCOLOMBIA	9	$444,500

LIQUIDACION DETALLADA DE APORTES

EMPLEADO			NOVEDADES																PENSION				SALUD				CCF				RIESGOS				PARAFISCALES				
No.	Identificación		Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vlp	Codigo	Dias	IBC	Aporte	Codigo	Dias	IBC	Aporte	Codigo	Dias	IBC	Aporte	Codigo	Dias	IBC	Aporte	Dias	IBC	Aporte	Exonerado SENA e ICBF	Total Aportes
1	CC	79906707	GODOY LOPEZ EDGAR ALFONSO							X											230201	30	$1,423,500	$227,800	EPS005	30	$1,423,500	$178,000	CCF21	30	$1,423,500	$28,500	14-4	30	$1,423,500	$7,500	30	$0	$0	No	$441,800
Total	Afiliados(1)																						$1,423,500	$227,800			$1,423,500	$178,000			$1,423,500	$28,500			$1,423,500	$7,500		$0	$0		$441,800

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
CC 79906707		GODOY LOPEZ EDGAR ALFONSO	INDEPENDIENTE	PRINCIPAL	CRA QUINTA # 2- 35 MANZANA 21 CASA 208	MOSQUERA-CUNDINAMARCA	8272125	No

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2025-11	2025-11	2000405053	9495008625	I	2025/12/02	2025/12/11	BANCOLOMBIA	9	$444,500

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 1)				1	$227,800	$1,300	$0	$229,100
PROTECCION	230201	800,229,739	0	1	$227,800	$1,300	$0	$229,100
ARL (ADMINISTRADORAS: 1)				1	$7,500	$100	$0	$7,600
COLPATRIA ARP	14-4	860,002,183	9	1	$7,500	$100	$0	$7,600
CCF (ADMINISTRADORAS: 1)				1	$28,500	$200	$0	$28,700
CAFAM	CCF21	860,013,570	3	1	$28,500	$200	$0	$28,700
EPS (ADMINISTRADORAS: 1)				1	$178,000	$1,100	$0	$179,100
SANITAS	EPS005	800,251,440	6	1	$178,000	$1,100	$0	$179,100
TOTAL				**1**	**$441,800**	**$2,700**	**$0**	**$444,500**

compensar | miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **NGEEK SAS**, identificada con **NI** número **900697738**, aportó por **JUAN PABLO MACIAS VARGAS**, identificado(a) con **CC** número **1032363649** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92105001** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

TIPO	CODIGO	NOMBRE	COTIZANTE	SUBTIPO	IRG	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRP	CORRECCION	DIAS	PERIODO	NÚMERO DE PLANILLA	FECHA DE PAGO	EXONERACION
Riesgos Laborales	14-11	ARL SURA	1	0															0		19	Noviembre - 2025	92105001	05/12/2025	S
Riesgos Laborales	14-11	ARL SURA	1	0												X			0		11	Noviembre - 2025	92105001	05/12/2025	S
Cajax	CCF24	Compensar Caja de Compensacion Fliar	1	0															0		19	Noviembre - 2025	92105001	05/12/2025	S
Cajax	CCF24	Compensar Caja de Compensacion Fliar	1	0												X			0		11	Noviembre - 2025	92105001	05/12/2025	S
Pensiones	230301	Porvenir	1	0															0		19	Noviembre - 2025	92105001	05/12/2025	S
Pensiones	230301	Porvenir	1	0												X			0		11	Noviembre - 2025	92105001	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0															0		19	Diciembre - 2025	92105001	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0												X			0		11	Diciembre - 2025	92105001	05/12/2025	S

El presente certificado se expide a los 2 días del mes Diciembre de 2025

Este documento está clasificado como privado por parte de Compensar Operador de Información

compensar | miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **NGEEK SAS**, identificada con **NI** número **900697738**, aportó por **JUAN PABLO MACIAS VARGAS**, identificado(a) con **CC** número **1032363649** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92105001** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

TIPO	CODIGO	NOMBRE	CONTANTE	SUBTIPO	IBC	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCE	IRP	CORRECCIÓN	DIAS	PERIODO	NÚMERO DE PLANILLA	FECHA DE PAGO	EXONERACIÓN
Riesgos Laborales	14-11	ARL SURA	1	0																0	19	Noviembre - 2025	92105001	05/12/2025	S
Riesgos Laborales	14-11	ARL SURA	1	0												X				0	11	Noviembre - 2025	92105001	05/12/2025	S
Cajas	CCF24	Compensar Caja de Compensacion Fiar	1	0																0	19	Noviembre - 2025	92105001	05/12/2025	S
Cajas	CCF24	Compensar Caja de Compensacion Fiar	1	0												X				0	11	Noviembre - 2025	92105001	05/12/2025	S
Pensiones	230301	Porvenir	1	0																0	19	Noviembre - 2025	92105001	05/12/2025	S
Pensiones	230301	Porvenir	1	0												X				0	11	Noviembre - 2025	92105001	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0																0	19	Diciembre - 2025	92105001	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0												X				0	11	Diciembre - 2025	92105001	05/12/2025	S

El presente certificado se expide a los 5 días del mes Diciembre de 2025

Este documento esta clasificado como privado por parte de Compensar Operador de Información.

compensar | miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **TSG THE IT EXPERTS SAS**, identificada con **NI** número **900994724**, aportó por **RONALD ALEXANDER CASTAÑEDA OLARTE**, identificado(a) con **CC** número **80195893** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92105012** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

TIPO	CODIGO	NOMBRE	COTIZANTE	SUBTIPO	IBC	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	VRP	CORRECCIÓN	DIAS	PERIODO	NÚMERO DE PLANILLA	FECHA DE PAGO	EXONERACIÓN
Riesgos Laborales	14-11	ARL SURA	1	0																0	19	Noviembre - 2025	92105012	05/12/2025	S
Riesgos Laborales	14-11	ARL SURA	1	0												X				0	11	Noviembre - 2025	92105012	05/12/2025	S
Caja	CCF24	Comfenalco Caja de Compensacion Fliar	1	0																0	19	Noviembre - 2025	92105012	05/12/2025	S
Caja	CCF24	Comfenalco Caja de Compensacion Fliar	1	0												X				0	11	Noviembre - 2025	92105012	05/12/2025	S
Pensiones	230301	Porvenir	1	0																0	19	Noviembre - 2025	92105012	05/12/2025	S
Pensiones	230301	Porvenir	1	0												X				0	11	Noviembre - 2025	92105012	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0																0	19	Diciembre - 2025	92105012	05/12/2025	S
Salud	EPS005	Sanitas EPS	1	0												X				0	11	Diciembre - 2025	92105012	05/12/2025	S

El presente certificado se expide a los 5 días del mes Diciembre de 2025

Este documento está clasificado como privado por parte de Compensar Operador de Información

compensar | miplanilla.com

CERTIFICADO DE APORTES AL SISTEMA DE PROTECCIÓN SOCIAL

Se certifica que **HEIMCORE SAS**, identificada con **NI** número **900425697**, aportó por **VICTOR MANUEL MENDOZA ANAYA,** identificado(a) con **CC** número **80113599** por concepto de aportes obligatorios al sistema General de Seguridad Social, mediante tipo de planilla **E** número **92099939** para el periodo de salud **2025-12** y pensiones **2025-11** de la siguiente forma.

CODIGO	NOMBRE	COTIZANTE	SUBTIPO	INC	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRP	COTIZACIÓN Y/O APORTE	DIAS	COTIZACIÓN Y/O APORTE	PERIODO	NUMERO DE PLANILLA	FECHA DE PAGO	ENDOSABLE
25-14	Administradora Colombiana de Pensiones - Colpensiones	1	0															0	$1.178.300	30	$1.178.300	Noviembre - 2025	92099939	19/12/2025	S
14-11	ARL SURA	1	0															0	$76.900	30	$76.900	Noviembre - 2025	92099939	19/12/2025	S
CCF24	Compensar Caja de Compensacion Fliar	1	0															0	$254.600	30	$254.600	Noviembre - 2025	92099939	19/12/2025	S
EPS017	Famisanar EPS Cafam Colsubsidio	1	0															0	$294.600	30	$294.600	Diciembre - 2025	92099939	19/12/2025	S

El presente certificado se expide a los 20 días del mes Diciembre de 2025

Este documento está clasificado como privado por parte de Compensar Operador de Información

Yeapdata

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA FUERZAS MILITARES – COGFM

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **UT273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente su compromiso de dar estricto cumplimiento a las políticas, lineamientos y directrices de seguridad informática definidas por las **Fuerzas Militares**, y en particular por la **Directiva de Seguridad Informática** vigente, en los siguientes términos:

- **Conocimiento de las políticas de seguridad informática:** El Contratista se compromete a **conocer** y estudiar integralmente las políticas de seguridad informática, así como la Directiva de Seguridad Informática de las Fuerzas Militares, incluyendo sus actualizaciones, anexos y lineamientos complementarios que sean comunicados de manera oficial por la Entidad.

- **Aceptación y cumplimiento de las políticas:** El Contratista declara que **acepta** expresamente las políticas de seguridad informática definidas por las Fuerzas Militares y se obliga a **ajustar sus actividades, entregas, procedimientos técnicos y administrativos** a lo establecido en dichas políticas, asegurando que todo el personal involucrado en la ejecución del contrato actúe en coherencia con las mismas.

- **Ajuste de procesos y controles internos:** El Contratista adoptará las medidas necesarias para **alinear sus procesos internos, controles de acceso, tratamiento de información, gestión de incidentes y manejo de activos de información** a las disposiciones contenidas en la Directiva de Seguridad Informática de las Fuerzas Militares, de manera que se preserve la **confidencialidad, integridad y disponibilidad** de la información y de los sistemas involucrados.

- **Difusión interna y responsabilidad del personal:** El Contratista se compromete a **socializar y difundir** las políticas de seguridad informática de las Fuerzas Militares entre el personal que participe en la ejecución del contrato, dejando claridad sobre sus responsabilidades individuales y colectivas en materia de seguridad de la información, y adoptando los mecanismos de seguimiento que sean necesarios para garantizar su cumplimiento.

- **Atención de requerimientos y auditorías:** El Contratista se obliga a **atender los requerimientos, revisiones, verificaciones o auditorías** que la Entidad o las instancias competentes definan en materia de seguridad informática, suministrando la información necesaria y facilitando las acciones de control que se consideren pertinentes, en el marco de la normativa aplicable.

- **Reporte de incidentes de seguridad:** El Contratista deberá **reportar de manera oportuna y por los canales establecidos** cualquier incidente, evento o situación que pueda comprometer la seguridad de la información, de los sistemas o de la infraestructura tecnológica asociada al objeto contractual, siguiendo los procedimientos definidos por la Directiva de Seguridad Informática de las Fuerzas Militares y las instrucciones del supervisor del contrato.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Hernando Tafur Lancheros

De: Orders Reply <O.Reply@f5.com>
Enviado el: lunes, 29 de septiembre de 2025 8:41 p. m.
Para: Compras; notificacionjudicial@cgfm.mil.co; Frank Gualdron; LATAMSOS
Asunto: FYI: F5 Networks - Order Number O-00034187 -



F5 Subscription A-S00030189: Order confirmation

Per your request, Subscription Number: A-S00030189 has been created via Order Number O-00034187.

If you did not request the subscription and this message is received in error, please contact F5 Networks and reference the order number in the subject line of this email.

If you ordered software-only products, your software fulfillment instructions will be sent in a separate email (as applicable).

Order Details:
Order Number: O-00034187
PO Number: 159-2025
Order Date: 2025-10-06
Subscription Number: A-S00030189
Subscription Start Date: 2025-10-06
Subscription End Date: 2027-10-05
Bill To Customer: Dacas Colombia SAS
Subscription Owner: COMANDO GENERAL DE LAS FUERZAS MILITARES

Line #	Part Number	Part Description	Qty
1.1	F5-V-O-ALL-BASE-PKG	Distributed Cloud Services Base Package (/mth) Org	1

1.2	F5-V-O-ADN-MSH-PUBLB	Distributed Cloud Mesh Globally Distributed Loadbalancer with Threat Campaigns (/mth) ADN Org	1
1.3	F5-V-O-ADN-MSH-PBVIP	Distributed Cloud Mesh Additional Anycast Virtual IP (VIP, /mth) ADN Org	2

Thank you,
The F5 team

This is an auto-generated email, please do not reply.

FOLLOW US

This email was sent by: F5 Networks, 801 5th Ave, Seattle, WA 98104 |
© F5 Networks, Inc. All rights reserved. |

COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

COMUNICACIÓN INTERNA

0125014300402

Al contestar cite este número
Radicado n° 0125014300402 / MDN-COGFM-JEMCO-SEMPE-CGDJ6-DITIN

Bogotá D.C., 13 octubre de 2025

Para: CGDJ2

De: DITIN

Asunto: Entrega ESP Contrato 259 de 2025.

Con toda atención, me permito enviar al señor Contralmirante jefe del Departamento Conjunto de Inteligencia y Contrainteligencia del Comando General de las Fuerzas Militares (CGDJ2), el estudio de seguridad del personal participante en el contrato 259 -2025 , para los trámites que ese departamento considere pertinentes.

Respetuosamente,

Mayor JOSE FRANCISCO LOMBANA CARDONA
Supervisor del contrato 259 de 2025

COMANDO GENERAL
FIEL COPIA TOMADA
DEL ORIGINAL
JFlorez John

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: CUMPLIMIENTO DE NORMAS DE SEGURIDAD INDUSTRIAL Y SALUD EN EL TRABAJO – CONTRATO NO. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **Unión Temporal UT273COGFM H&Y 2025**, en calidad de **Contratista**, manifiesta formalmente su compromiso de **garantizar la correcta prestación del Servicio de Suscripción WAF – Lote No. 5**, conforme a los términos, condiciones y **acuerdos de nivel de servicio (ANS)** establecidos.
Durante la ejecución del contrato, el contratista dio estricto cumplimiento a las **normas de seguridad industrial y salud en el trabajo**, garantizando que todas las actividades desarrolladas se realizaran bajo **condiciones seguras y controladas**.

Se veló por la **integridad física del personal técnico y operativo**, mediante la aplicación de los protocolos establecidos en el **Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)**, el **uso adecuado de elementos de protección personal (EPP)** y la **implementación de medidas preventivas** para minimizar los riesgos laborales.

Asimismo, se aseguró el **cumplimiento de los lineamientos de seguridad** establecidos por la entidad contratante, manteniendo un **ambiente laboral seguro** durante las fases de transporte, instalación, configuración y pruebas de los equipos.

En consecuencia, la **Unión Temporal UT273COGFM H&Y 2025** acredita el **cumplimiento de las obligaciones en materia de seguridad industrial y salud en el trabajo**, conforme a la normatividad aplicable y a los compromisos contractuales adquiridos.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: GARANTÍA DE SOPORTE DEL FABRICANTE Y SERVICIO DE SOPORTE ESPECIALIZADO

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025**, la **UT 273COGFM H&Y 2025**, en calidad de Contratista, se compromete a garantizar el soporte del fabricante y el servicio de soporte especializado para la solución de ciberseguridad descrita en el presente anexo, en los términos que se indican a continuación:

1. Garantía de soporte del fabricante 7x24

La UT 273COGFM H&Y 2025 garantiza el **soporte del fabricante en esquema 7x24** (siete días a la semana, veinticuatro horas al día) durante **dos (2) años**, contados a partir del **06 de octubre de 2025** o desde la fecha que indique la plataforma o el documento oficial emitido por el fabricante.

El soporte del fabricante deberá incluir, como mínimo:

- Soporte vía **correo electrónico**.
- Soporte vía **telefónica**.
- **Recepción de alertas, mensajes o noticias** sobre las actualizaciones del servicio durante el periodo contratado.
- **Sin límite** en la cantidad de apertura de casos, incidentes, solicitudes, requerimientos, consultas, soporte técnico y resolución de problemas.

2. Servicio de soporte 7x24 de la UT 273COGFM H&Y 2025

Adicionalmente, la UT 273COGFM H&Y 2025 se compromete a prestar **soporte 7x24** durante **dos (2) años**, contados a partir del **06 de octubre de 2025** o desde la fecha que indique la plataforma o el documento del fabricante, en concordancia con lo establecido en el numeral anterior.

El soporte deberá incluir, como mínimo:

- Apoyo en **nuevas configuraciones** de la solución.
- **Atención de incidentes** a través de correo electrónico, teléfono y mesa de ayuda.
- **Instalación de nuevas actualizaciones** de la solución, cuando aplique y previa validación técnica.
- Realización de por lo menos **un (1) mantenimiento general al año** sobre la solución.
- Atención de **casos de carácter técnico en temas funcionales** de las diferentes aplicaciones que estén siendo protegidas por la solución de ciberseguridad objeto del presente anexo.

3. Tiempos de respuesta y atención en sitio

El servicio de soporte deberá ser atendido conforme a los siguientes tiempos:

- Si en el lapso de **cuatro (4) horas** después de haber sido reportado un incidente **no se ha dado una solución definitiva** al mismo, la UT 273COGFM H&Y 2025 deberá **enviar personal técnico especializado a sitio** en un tiempo máximo de **dos (2) horas** adicionales.
- El servicio de soporte se podrá brindar a través de **herramientas de servicio remoto**, o también **en sitio en la ciudad de Bogotá D.C.**, de acuerdo con la naturaleza del incidente y las instrucciones del supervisor del contrato.

4. Procedimiento de escalamiento y gestión de tickets

El servicio de soporte brindado deberá contemplar un **procedimiento de escalamiento**, el cual se aplicará cuando la complejidad o el impacto del incidente así lo requiera. Este procedimiento se gestionará mediante la **apertura y seguimiento de un ticket de servicio** por cada incidente presentado, dejando registro de:

- Fecha y hora de apertura del ticket.
- Descripción del incidente.
- Acciones realizadas.
- Nivel de escalamiento.
- Cierre y solución definitiva del caso.

5. Atención ilimitada de casos y alcance del soporte

La UT 273COGFM H&Y 2025 se compromete a prestar una **atención ilimitada** a los casos reportados por el **COGFM**, referentes a cualquier evento relacionado con:

- El **funcionamiento** de los sistemas, equipos o plataformas descritas en el presente anexo.
- La **administración** de la solución.
- La **gestión de incidentes** o eventos de seguridad.

La atención se mantendrá **hasta dejar en normal y completo funcionamiento** el sistema o herramienta de ciberseguridad, garantizando la continuidad operativa y la protección adecuada de la información y de los servicios involucrados.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE SOPORTE 24x7 DE LA SOLUCIÓN

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. CONTRATO 259COGFM DIADF 2025**, la **UT 273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente su compromiso de garantizar el servicio de soporte de la solución en los términos que se describen a continuación:

1. **Disponibilidad y canales de soporte**

La solución contará con **soporte 24x7** (las 24 horas del día, los 7 días de la semana), prestado a través de, como mínimo, los siguientes medios de contacto:

- Teléfono.
- Correo electrónico (mail).
- Otros medios de contacto autorizados por la Entidad y definidos como canales oficiales de soporte.

2. **Idioma y franja horaria de atención**

El servicio de soporte deberá permitir la **interacción con el Centro de Soporte en idioma español**, garantizando la atención en el **uso horario de la región (Colombia)** durante el **horario laboral**, de acuerdo con las necesidades operativas y las solicitudes que formule el supervisor del contrato.

3. **Acuerdos de Nivel de Servicio (SLA)**

El Contratista se compromete a cumplir los siguientes **SLAs** asociados a la solución y al servicio de soporte técnico:

3.1. Disponibilidad de la plataforma

- La plataforma SaaS deberá proporcionar una **disponibilidad mínima del 99,99 %**, medida sobre la base mensual, excluyendo únicamente las ventanas de mantenimiento previamente acordadas con la Entidad.

3.2. Tiempo de respuesta del soporte técnico

- El servicio de soporte técnico de la solución propuesta deberá garantizar un **tiempo de respuesta máximo de treinta (30) minutos** para el **primer contacto** con el usuario o con el equipo designado por la Entidad, contado a partir del registro del incidente o requerimiento en los canales oficiales de soporte.

3.3. Análisis de causa raíz de incidentes

El servicio de soporte técnico deberá cumplir el siguiente SLA para el análisis de causa raíz de incidentes:

- **Incidente de severidad crítica**:
    - Presentar un **borrador (draft)** del análisis de causa raíz en un tiempo máximo de **veinticuatro (24) horas** contadas a partir de la apertura del incidente.
    - Entregar el **análisis de causa raíz final** en un tiempo máximo de **siete (7) días calendario**.

Yeapdata®

Heimcore

4. Obligaciones del Contratista

El Contratista se compromete a:

- Mantener disponibles y operativos los canales de soporte definidos.
- Asegurar que el personal de soporte cuente con las competencias técnicas necesarias y dominio del idioma español.
- Atender de manera oportuna y adecuada las solicitudes, incidentes o requerimientos reportados por la Entidad, de acuerdo con los SLAs establecidos en el presente documento y en el contrato principal.
-

En constancia de lo anterior, se firma el presente documento para los fines pertinentes.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS SOLUCIÓN DE SEGURIDAD (WAF / FILTRADO Y ANÁLISIS WEB/PROXY)

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025**, la **UT 273COGFM H&Y 2025**, en calidad de Contratista, se compromete a realizar los **mantenimientos preventivos y correctivos** de la solución de seguridad descrita en el presente anexo (WAF / solución de seguridad de filtrado y análisis web/proxy), en los siguientes términos:

1. Mantenimientos preventivos

El Contratista deberá efectuar como mínimo **dos (2) mantenimientos preventivos** a la solución descrita en el presente anexo, durante el término de la garantía.
Estos mantenimientos preventivos deberán incluir, como mínimo, las siguientes actividades:

1.1. Actualizaciones y parches de seguridad
- Aplicación de **actualizaciones y parches de seguridad críticos** en el WAF.
- Revisión periódica de las **nuevas versiones del WAF** y su impacto en la configuración actual.

1.2. Revisión y solución de errores
- Monitoreo y **resolución de errores o fallos en las reglas de seguridad**.
- Identificación y mitigación de **falsos positivos y falsos negativos** en la protección del WAF.

1.3. Copias de seguridad y recuperación
- Programación y validación de **copias de seguridad** de configuraciones y reglas de seguridad.
- Definición y prueba de un **plan de recuperación** en caso de incidentes o errores de configuración.

1.4. Monitoreo y análisis de logs
- Revisión periódica de **logs de actividad y eventos de seguridad**.
- Generación de **reportes sobre ataques detectados** y acciones de mitigación aplicadas.

1.5. Optimización de recursos

- Análisis del **consumo de recursos en la nube** y optimización de configuraciones.
- Ajustes en las **reglas de caching y mitigación de ataques** para mejorar la disponibilidad y el rendimiento del servicio.

1.6. Desactivación de funcionalidades inoperativas

- Identificación y eliminación de **reglas o configuraciones obsoletas o ineficaces**.
- Mantenimiento de una **configuración optimizada**, basada en buenas prácticas.

1.7. Procedimientos de hardening

- Implementación de **medidas de refuerzo de seguridad (hardening)** recomendadas por los principales proveedores de WAF en la nube.
- Configuración avanzada de mitigación de amenazas (por ejemplo: **Rate Limiting, Bot Management, Geo-blocking**, entre otras).

1.8. Nuevas implementaciones

- Implementación de **nuevas funcionalidades o ajustes** requeridos para mejorar la efectividad de la solución, de acuerdo con las necesidades del COGFM y las recomendaciones del fabricante.

2. Programación de ventanas de mantenimiento

Las **ventanas de mantenimiento** deberán ser programadas en **horarios no hábiles**, previa coordinación y aprobación del **Supervisor del contrato**, y de acuerdo con las necesidades operativas del **COGFM**, procurando minimizar el impacto en la prestación del servicio.

3. Acompañamientos y mantenimientos correctivos

En caso de presentarse **fallas en la solución de seguridad** descrita en el presente anexo, el Contratista se compromete a efectuar los **acompañamientos todas las veces que se requiera**, los cuales deberán incluir, como mínimo:

- **Reemplazo de la solución de seguridad** por otra de **iguales o superiores características** cuando sea necesario.
- **Instalación y/o reparación de software** asociado a la solución.
- **Configuraciones, puesta en producción y verificación de funcionamiento** de la solución, hasta lograr la normalización completa del servicio.

El servicio será brindado **en sitio en la ciudad de Bogotá D.C.**, de acuerdo con los tiempos de respuesta establecidos contractualmente.

El **tiempo máximo permitido para el cambio o reparación de la solución de seguridad** será de **veinte (20) días calendario** contados a partir del reporte del incidente. En caso de que la falla genere **afectación del servicio**, el Contratista deberá:

- **Suministrar, configurar y poner en funcionamiento temporalmente** una solución de **iguales o superiores características técnicas**,
- Sin costo adicional para el **COGFM**,

- Hasta tanto se dé solución definitiva a la novedad o incidente reportado, garantizando la **continuidad en la prestación de los servicios**.

4. Continuidad del servicio y obligaciones adicionales

El Contratista deberá:

- **Suministrar, configurar y poner en perfecto funcionamiento la solución de seguridad** después de realizar cada mantenimiento (cuando aplique), garantizando la continuidad de los servicios.
- En caso de que la solución de seguridad requiera la **reinstalación o reconfiguración de software, sistema operativo o firmware**, estas labores deberán ser realizadas por el Contratista **sin costo adicional para el COGFM**.
- Asumir **todos los gastos** que se ocasionen por concepto de **transporte y otros costos asociados** necesarios para cumplir con los mantenimientos preventivos y correctivos, sin trasladar dichos costos al COGFM.

Asimismo, el Contratista se compromete a prestar **atención ilimitada** a los casos reportados por el **COGFM**, referentes a cualquier evento relacionado con el **funcionamiento, administración, incidentes o eventos de seguridad** de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en **normal y completo funcionamiento** el sistema o herramienta de ciberseguridad.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE EJECUCIÓN A TODO COSTO Y ALCANCE DEL SERVICIO

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025, la UT 273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente que la ejecución del contrato se realizará **a todo costo**, entendiendo por ello que serán de su exclusiva responsabilidad todos los gastos, recursos, actividades, personal, herramientas, licencias, materiales y demás elementos necesarios para la correcta prestación del servicio.
El Contratista se compromete a:

1. **Prestar el servicio objeto del contrato** incluyendo, de manera integral, las actividades de **instalación, configuración, implementación y puesta en marcha** de la solución contratada.
2. **Realizar las pruebas de funcionalidad necesarias** para verificar el correcto desempeño de la solución, dejando evidencia de las **pruebas exitosas de funcionalidad** y asegurando que el servicio quede plenamente operativo conforme a las especificaciones técnicas y a los requerimientos del supervisor del contrato.
3. Asumir todos los costos y recursos requeridos para atender las obligaciones aquí descritas, sin que ello genere costos adicionales para la Entidad Contratante, salvo los expresamente pactados en el contrato principal.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE CIBERDEFENSA Y SEGURIDAD DE LA INFORMACIÓN MINISTERIO DE DEFENSA – COMANDO GENERAL DE LAS FUERZAS MILITARES

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **UT273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente su compromiso de **cumplir lo expuesto en las políticas y directivas de ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares**, durante el tiempo de **ejecución, garantía y soporte** que brindará en el marco del contrato.

Para tal fin, el Contratista se compromete a ajustar sus procesos técnicos y administrativos a dichos lineamientos, a socializar estas obligaciones con el personal involucrado en la ejecución del contrato y a adoptar las medidas necesarias para proteger la información y la infraestructura tecnológica asociada, incluyendo el **reporte oportuno de incidentes o eventos de seguridad** a través de los canales definidos por la Entidad.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE ACTUALIZACIONES DE LA SOLUCIÓN DE SEGURIDAD

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025**, la **UT 273COGFM H&Y 2025**, en calidad de Contratista, se compromete a realizar la gestión de **actualizaciones de la solución de seguridad** descrita en el presente anexo, en los siguientes términos:

Durante el tiempo de la **garantía**, el Contratista deberá **brindar e instalar actualizaciones** a la solución de seguridad, cada vez que se libere en el mercado una **nueva versión de software, *upgrade* o parche**, emitido por el fabricante y aplicable a la solución implementada.

La instalación de dichas actualizaciones se realizará:

- **Previa solicitud y aprobación** del supervisor del contrato.
- **Una vez hayan sido probadas en laboratorio**, ya sea por el fabricante o por el Contratista, con el fin de verificar su estabilidad y compatibilidad.
- Asegurando en todo momento la **continuidad del servicio** y el correcto **funcionamiento de los sistemas** asociados a la solución de seguridad.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA FUERZAS MILITARES – COGFM

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **UT273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente su compromiso de dar estricto cumplimiento a las políticas, lineamientos y directrices de seguridad informática definidas por las **Fuerzas Militares**, y en particular por la **Directiva de Seguridad Informática** vigente, en los siguientes términos:

- **Conocimiento de las políticas de seguridad informática:** El Contratista se compromete a **conocer** y estudiar integralmente las políticas de seguridad informática, así como la Directiva de Seguridad Informática de las Fuerzas Militares, incluyendo sus actualizaciones, anexos y lineamientos complementarios que sean comunicados de manera oficial por la Entidad.

- **Aceptación y cumplimiento de las políticas:** El Contratista declara que **acepta** expresamente las políticas de seguridad informática definidas por las Fuerzas Militares y se obliga a **ajustar sus actividades, entregas, procedimientos técnicos y administrativos** a lo establecido en dichas políticas, asegurando que todo el personal involucrado en la ejecución del contrato actúe en coherencia con las mismas.

- **Ajuste de procesos y controles internos:** El Contratista adoptará las medidas necesarias para **alinear sus procesos internos, controles de acceso, tratamiento de información, gestión de incidentes y manejo de activos de información** a las disposiciones contenidas en la Directiva de Seguridad Informática de las Fuerzas Militares, de manera que se preserve la **confidencialidad, integridad y disponibilidad** de la información y de los sistemas involucrados.

- **Difusión interna y responsabilidad del personal:** El Contratista se compromete a **socializar y difundir** las políticas de seguridad informática de las Fuerzas Militares entre el personal que participe en la ejecución del contrato, dejando claridad sobre sus responsabilidades individuales y colectivas en materia de seguridad de la información, y adoptando los mecanismos de seguimiento que sean necesarios para garantizar su cumplimiento.

- **Atención de requerimientos y auditorías:** El Contratista se obliga a **atender los requerimientos, revisiones, verificaciones o auditorías** que la Entidad o las instancias competentes definan en materia de seguridad informática, suministrando la información necesaria y facilitando las acciones de control que se consideren pertinentes, en el marco de la normativa aplicable.

- **Reporte de incidentes de seguridad:** El Contratista deberá **reportar de manera oportuna y por los canales establecidos** cualquier incidente, evento o situación que pueda comprometer la seguridad de la información, de los sistemas o de la infraestructura tecnológica asociada al objeto contractual, siguiendo los procedimientos definidos por la Directiva de Seguridad Informática de las Fuerzas Militares y las instrucciones del supervisor del contrato.

.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

	12 DICIEMRBE 2025		BOGOTÁ D.C

COMANDO GENERAL DE LAS FUERZAS MILITARES
JOSE FRANCISCO LOMBANA CARDONA
316 5775377
Carrera 54 N°26-25 Barrio Esmeralda Bogotá

ACTA TRANSFERENCIA DE CONOCIMIENTOS

OBJETO DE CONTRATO

El contratista se obliga para con EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a prestar el servicio de mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 LOTE 2: LICENCIAS PROXY WEB ;LOTE 3: SUSCRIPCIÓN PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato.

TRANSFERENCIA DE CONOCIMIENTO LOTE 3 - SUSCRIPCIÓN PROTECCIÓN DE DATOS

En cumplimiento de las **obligaciones contractuales** establecidas en el **Contrato 259COGFM DIADF 2025**, el presente apartado introduce la **transferencia de conocimiento** orientada a asegurar que el equipo designado cuente con los fundamentos técnicos y operativos para administrar Falcon CrowdStrike de forma autónoma y continua.

Registro Fotográfico Transferencia de Conocimeinto





Yeapdata®

Heimcore

PLANILLA ASISTENCIA

INTEGRANTES SESIÓN DE SUSCRIPCIÓN DE PROTECCIÓN DE DATOS				
ITEM	**NOMBRES Y APELLIDOS**	**CEDULA**	**TELEFONO**	**FIRMA**
1	Erika Rocha	1098136444	3153149793	
2	Fabian Rodriguez Gomez	94507989	3207126589	
3	Wilson Vargas Cordoba	1070961061	3102473445	

TEMARIO DE TRANSFERENCIA DE CONOCIMEINTOS – SUSCRIPCIÓN DE PROTECCIÓN DE DATOS

Duración total: 40 horas
Modalidad: Teórico

Objetivo general:

La capacitación en Falcon CrowdStrike tiene como objetivo dejar al equipo en capacidad de operar y administrar la plataforma de forma autónoma, abarcando la configuración inicial de la consola, el despliegue y verificación del sensor en endpoints y servidores, la creación y ajuste de políticas de protección, la gestión de hosts y la visibilidad operacional, así como la detección, análisis y respuesta ante incidentes mediante capacidades EPP/Antimalware, EDR/XDR y respuesta en tiempo real, complementado con prácticas de caza de amenazas y lineamientos de protección de datos, orientados a fortalecer la postura de ciberseguridad y asegurar una operación continua y controlada.

A continuación, se relaciona el detalle de cada una de las sesiones:

- **Sesión 1 (4h) – Visión general y fundamentos**
  - Alcance del proyecto y objetivos operativos del SOC/área responsable.
  - Conceptos: EPP vs EDR vs XDR, telemetría, detección por comportamiento.
  - Arquitectura Falcon (Console, Sensor, módulos) y flujo de eventos.
  - Recorrido guiado por la consola: menús clave, vistas principales y buenas prácticas de navegación.

- **Sesión 2 (4h) – Configuración inicial y preparación operativa**
  - Creación/ajuste de **roles y permisos** (admin, analista, auditor) y segregación de funciones.
  - Parametrización base: alertas, notificaciones, retención/visibilidad (según licencia).

- Reglas básicas de operación: naming convention, control de cambios y checklist de alistamiento.
- Validación de prerequisitos y criterios de "plataforma lista para operar".

- **Sesión 3 (4h) – Despliegue del Sensor en Windows**
  - Métodos de instalación: manual, por herramientas de despliegue (GPO/SCCM/Intune u otras).
  - Paquetes, tokens/installer, verificación de instalación y comunicación con la nube.
  - Manejo de errores frecuentes (proxy, DNS, certificados, restricciones de red).
  - Laboratorio: instalación en un grupo piloto y validación de reporting en consola

---

- **Sesión 4 (4h) – Despliegue del Sensor en Linux y servidores**
  - Instalación en distribuciones Linux (paquetes, servicios, permisos) y consideraciones en servidores.
  - Actualización/versionamiento del sensor y política de mantenimiento.
  - Validación de telemetría, salud del host y diagnóstico de conectividad.
  - Laboratorio: despliegue en servidor Linux y checklist de "host protegido".

- **Sesión 5 (4h) – Gestión de Hosts e inventario**
  - Inventario: estados del sensor, cobertura, etiquetas y clasificación por criticidad.
  - Creación de **grupos** por área de negocio/entorno (producción, pruebas, usuarios).
  - Acciones remotas básicas sobre hosts (aislamiento, contención, recolección de info según permisos).
  - Rutina diaria: revisión de salud, endpoints sin sensor, endpoints inactivos y recomendaciones.

- **Sesión 6 (4h) – Políticas de protección y afinamiento**
  - Estructura de políticas: prevención, comportamiento, control de ejecución (según módulos).
  - Asignación por grupos y estrategia "baseline + excepciones controladas".
  - Gestión de exclusiones: criterios, trazabilidad, vigencia y revisión periódica.
  - Taller: creación de política para endpoints y otra para servidores + plan de tuning.

- **Sesión 7 (4h) – Antivirus/Antimalware y prevención**
  - Configuración de prevención y respuesta ante malware (bloqueo, cuarentena, remediación).
  - Gestión de falsos positivos: validación, evidencia, ajuste de exclusiones con control.
  - Pruebas controladas (no disruptivas) para validar detección y respuesta.
  - Recomendaciones para mantener equilibrio entre seguridad y operación.

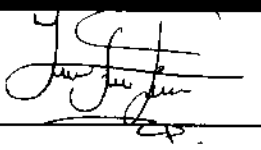
- **Sesión 8 (4h) – Detección y respuesta EDR/XDR**
  - Interpretación de detecciones: severidad, táctica/técnica, contexto del endpoint.
  - Correlación y análisis: línea de tiempo, procesos, indicadores y evidencia.
  - Acciones de contención: aislamiento del host, bloqueo, medidas inmediatas.
  - Introducción práctica a RTR (respuesta en tiempo real): uso responsable y registros.

- **Sesión 9 (4h) – Respuesta a incidentes (end-to-end)**
  - Flujo estándar: triage → contención → erradicación → recuperación → lecciones aprendidas.
  - Gestión de casos: documentación, evidencias, responsables y criterios de cierre.
  - Escenarios: ransomware, credenciales comprometidas, ejecución sospechosa, lateral movement.

- Taller: atención de un incidente simulado y elaboración de resumen ejecutivo.

- **Sesión 10 (4h) – Threat Hunting, protección de datos y reporting**
  - Metodología de caza: hipótesis, consultas/búsquedas, priorización de hallazgos.
  - Enfoque de protección de datos: monitoreo de eventos relevantes y recomendaciones (según capacidades licenciadas).
  - Dashboards y reportes: operativos y ejecutivos (cobertura, tendencias, tiempos de respuesta).
  - Cierre: checklist de operación, plan de mejora continua y próximos pasos (madurez SOC).

Cordialmente,

Por COGFM		
My Jose Lombana Cardona		12-12-2025

Por UT 273COGFM H&Y 2025		
Carlos Giovani Díaz Rueda		12/12/2025

CERTIFICATE

OF COMPLETION

This certifies that

Wilson O. Vargas

has successfully completed the
CrowdStrike Certified Falcon Administrator (CCFA)
conducted CrowdStrike University
on November 24, 2025

Nathan Cole
Chief Executive Officer

Aaron Loeb
Training Coordinator

CERTIFICATE

OF COMPLETION

This certifies that

Enuar E. Roales

has successfully completed the
CrowdStrike Certified Falcon Administrator (CCFA)
conducted CrowdStrike University
on November 24, 2025

Nathan Cole
Chief Executive Officer

Aaron Loeb
Training Coordinator

CERTIFICATE

OF COMPLETION

This certifies that

Idier Loaiza Zabala

has successfully completed the
CrowdStrike Certified Falcon Administrator (CCFA)
conducted CrowdStrike University
on November 24, 2025

Nathan Cole
Chief Executive Officer

Aaron Loeb
Training Coordinator

CERTIFICATE

OF COMPLETION

This certifies that

Fabián J. Rodriguez

has successfully completed the
CrowdStrike Certified Falcon Administrator (CCFA)
conducted CrowdStrike University
on November 24, 2025

Nathan Cole
Chief Executive Officer

Aaron Loeb
Training Coordinator

CROWDSTRIKE

Order Number 00344555
Account Name Comando General de las Fuerzas Militares
Account Address Carrera 59a N°44 b-29 Barrio Esmeralda, Bogota, , 111071 Colombia

Dear Valued Customer,

I am pleased to inform you that your CrowdStrike purchase order has been fully processed. Please find a summary of your order below:

Product Name	Order Quantity	Start Date	End Date
Falcon Endpoint Protection Enterprise Bundle	1400.00	10/31/2025	11/1/2027
Threat Graph Standard	1400.00	10/31/2025	11/1/2027
Prevent	1400.00	10/31/2025	11/1/2027
Insight	1400.00	10/31/2025	11/1/2027
Falcon Firewall Management	1400.00	10/31/2025	11/1/2027
Falcon Device Control	1400.00	10/31/2025	11/1/2027
Overwatch	1400.00	10/31/2025	11/1/2027
CrowdStrike Falcon Intelligence	1400.00	10/31/2025	11/1/2027
Identity Threat Protection (Accounts)	1400.00	10/31/2025	11/1/2027
Falcon Spotlight	1400.00	10/31/2025	11/1/2027
Discover	1400.00	10/31/2025	11/1/2027
Falcon Next-Gen SIEM Additional Ingestion (qty = GB)	65.00	10/31/2025	11/1/2027
Falcon Next-Gen SIEM 90 Day Retention (qty = GB)	75.00	10/31/2025	11/1/2027
Falcon Search Retention - 180 days	1400.00	10/31/2025	11/1/2027
Falcon Search Retention - 365 days	1.00	10/31/2025	11/1/2027
Charlotte AI	1400.00	10/31/2025	11/1/2027
Charlotte AI Additional Usage (qty=350 credits/month)	1.00	10/31/2025	11/1/2027
CrowdStrike Falcon Certification Program Exam Voucher	4.00	10/31/2025	10/30/2026
Falcon Data Protection for Endpoint	1400.00	10/31/2025	11/1/2027
Essential Support	1.00	10/31/2025	11/1/2027

CrowdStrike Technical Support can be reached via: support@crowdstrike.com

If you have questions regarding this Order confirmation contact your sales representative.

All Orders are subject to and governed by the terms and conditions located here unless CrowdStrike and the Partner identified above have otherwise executed an agreement, in which case, that agreement governs the Order. All products and services are provided subject to the end user terms and conditions located here. In the event that a P.O. is required for invoicing and has not already been provided, Partner shall immediately provide the P.O. to CrowdStrike. Otherwise, Partner agrees to pay an invoice without a P.O. reference. Any terms and conditions on a P.O., or that are specified in any email from Partner or Customer or in response to this confirmation, are void and have no legal effect.

Thank You

150 Mathilda Place . Suite 300 . Sunnyvale . CA . 94086
T : @CROWDSTRIKE W : CROWDSTRIKE.COM

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: SOPORTE Y GARANTÍA TÉCNICA DE LA SUSCRIPCIÓN DE PROTECCIÓN DE DATOS

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **UT273COGFM H&Y 2025**, en calidad de Contratista, establece la siguiente **garantía técnica y esquema de servicio de soporte** para la **Suscripción de Protección de Datos**, con el fin de asegurar su adecuada operación, continuidad y disponibilidad durante la vigencia del contrato.

1. Soporte del fabricante

El fabricante de la Suscripción de Protección de Datos deberá brindar soporte en un horario de **24x7** (las 24 horas del día, los 7 días de la semana), a partir de la firma del contrato y por una vigencia de **veinticuatro (24) meses**. Como mínimo, se deberá garantizar:

- Acceso al **portal de soporte**, incluyendo base de conocimiento y mecanismos de creación y escalamiento de *tickets*.
- Soporte telefónico **7x24x365**.
- **Priorización de casos**, de acuerdo con la criticidad e impacto en la operación del servicio.
- Asignación de un **TAM (Technical Account Manager / especialista de producto)** para revisión y evaluación periódica de la suscripción y de la plataforma de protección de datos.
- Realización de **healthcheck de la solución de forma trimestral**, con recomendaciones de ajuste y mejora.
- Emisión de **reportes trimestrales** del estado de la solución, incidentes, tendencias y acciones preventivas.
- **Gestión de casos proactivos**, orientados a prevenir incidentes y optimizar el uso de la suscripción.
- **Acompañamiento en nuevas funcionalidades y actualizaciones** que se liberen para la Suscripción de Protección de Datos.
- **Acompañamiento en el Kick Off del proyecto**, para asegurar la correcta configuración inicial y alineación con los requerimientos del COGFM.

2. Tiempos de respuesta del soporte

El servicio de soporte deberá ser atendido de manera **inmediata**, de acuerdo con lo solicitado por el supervisor del contrato. Se establecen los siguientes tiempos máximos:

- **Tiempo máximo de respuesta:** hasta **dos (2) horas** después de haber sido reportado
- el incidente.
- De ser necesario, el proveedor deberá **enviar personal técnico especializado a sitio** en un tiempo máximo de **cuatro (4) horas** contadas a partir del reporte del incidente.
- El **tiempo máximo permitido para restablecer el servicio** será de **cuatro (4) horas**, contadas desde la apertura del caso, salvo eventos de fuerza mayor debidamente justificados y aceptados por el supervisor del contrato.

3. Tipos de atención del soporte

El esquema de atención del soporte se prestará bajo los siguientes niveles:

3.1. Soporte Nivel 1

- Atención de manera **presencial, dos (2) días a la semana**, con una duración de **ocho (8) horas laborales por día (2x8)**.
- La atención se realizará en las instalaciones del **Comando General de las Fuerzas Militares – Centro Administrativo Nacional (CAN), Edificio Fortaleza, Carrera 54 # 26-25, ciudad de Bogotá D.C.**
- El **horario de trabajo** será definido de acuerdo con el requerimiento del **supervisor del contrato**.

3.2. Soporte Nivel 2

- Atención, cuando se requiera, por medio **telefónico** o de manera **remota**, a través de herramientas web *online*.
- La prestación se realizará en horario **7x24** (7 días a la semana, 24 horas al día), durante la vigencia de ejecución del contrato.
- El servicio deberá cumplir los **términos y tiempos de respuesta** definidos en el presente documento y en los acuerdos de nivel de servicio que se adopten.

Yeapdata®

Heimcore

4. Garantía de soporte

Como parte de la garantía técnica asociada a la Suscripción de Protección de Datos, se establece que:

- El Contratista deberá **garantizar el normal funcionamiento de la solución** después de la implementación y puesta en marcha.
  En caso de presentarse fallas atribuibles a la implementación, configuración o parametrización, el Contratista deberá **asumir los gastos** necesarios (configuraciones adicionales, horas de ingenieros, visitas a sitio, entre otros) que se generen hasta restablecer el funcionamiento de la solución, en un tiempo no mayor a **veinticuatro (24) horas**.
- El soporte deberá estar disponible los **365 días del año**, en horario **7x24** (7 días a la semana, 24 horas al día).
- El servicio de soporte deberá ser atendido de manera **inmediata** a través de:
  - Una **línea telefónica gratuita**,
  - Servicio de **correo electrónico**, y/o
  - Atención **remota**,
  -

Conforme a los niveles de servicio acordados.

- En caso de que, en un lapso de **cuatro (4) horas** después de haber sido reportado el incidente, **no se haya dado solución** al mismo, el Contratista deberá **enviar personal técnico especializado a sitio** en un tiempo máximo de **dos (2) horas** adicionales, manteniendo la atención hasta el restablecimiento total de la suscripción y de la operación normal del servicio de protección de datos.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

FALCON SPOTLIGHT

Un nuevo enfoque para la gestión de vulnerabilidades

La solución más rápida y sencilla para reducir el riesgo y la exposición, cubrir los vacíos de seguridad y estar mejor preparado para responder a los ataques

FALCON SPOTLIGHT

GESTIÓN DE VULNERABILIDADES INSTANTÁNEA Y SIN ESCANEOS

CrowdStrike® Falcon Spotlight™ les ofrece a los equipos de seguridad una evaluación en tiempo real, y siempre actualizada, de la exposición a vulnerabilidades de sus endpoints. La integración nativa del Falcon Spotlight en la plataforma Falcon® de CrowdStrike les permite a los clientes gestionar las vulnerabilidades dentro de un marco completo de protección de endpoints. Falcon Spotlight añade preparación y prontitud a la inigualable prevención, detección y respuesta de la plataforma Falcon, lo que resulta en una postura de seguridad más fuerte y una protección contra las brechas incomparable.

- **Protección Integrada:** Spotlight es un componente clave de la plataforma integral y unificada de protección para endpoints de CrowdStrike. Con Spotlight y la plataforma Falcon, usted no solo puede ver sus vacíos de seguridad, sino, también, a cuáles de éstos les están apuntando sus adversarios. Esto le permite armarse con la protección proactiva que se necesita para bloquear ataques avanzados.
- **Visibilidad Integral:** Spotlight no requiere escaneos ni agentes nuevos para su implementación y manejo - solo tiene que prenderlo y empezar a ver los resultados. Spotlight le brinda visibilidad en toda su empresa, independientemente de si los endpoints son físicos o virtuales, on u off-premise, o móviles. Usted recibe una visibilidad incomparable sobre las vulnerabilidades en todos sus negocios distribuidos, sin afectaciones.
- **Sencillo:** Spotlight ofrece, continuamente, una información que está siempre actualizada, poniéndola en manos de los analistas de seguridad. Esto le ayuda a mejorar el tiempo de respuesta, reduciendo el esfuerzo que implica comprender su postura de seguridad y volverse más proactivo.
- **Cero impacto:** la arquitectura nativa de la nube de CrowdStrike permite tener una visibilidad constante sobre las vulnerabilidades de los endpoints, sin necesidad de realizar complicados escaneos de red o host que demanden un gran uso de recursos.

PRINCIPALES BENEFICIOS

Falcon Spotlight ofrece una gestión de vulnerabilidades sin escaneos. Construido sobre la plataforma Falcon, éste ofrece evaluaciones oportunas y sin impacto de la postura de seguridad de endpoints, así como acceso bajo demanda a los resultados. Esto les permite a los equipos de seguridad reducir el riesgo y tomar mejores decisiones de manera más rápida.

Brinda una protección integral que cierra las brechas entre la gestión de vulnerabilidades y la prevención de amenazas

Ofrece una implementación fácil y nativa de la nube que no requiere agentes adicionales o nueva infraestructura

Ofrece información oportuna y actualizada bajo demanda

Provee evaluaciones sin impacto y sin escaneos

FALCON SPOTLIGHT

PRINCIPALES CAPACIDADES DEL PRODUCTO

Falcon Spotlight resuelve los desafíos que afectan a las soluciones tradicionales de gestión de vulnerabilidades, ofreciendo los siguientes beneficios:

INTEGRACION PERFECTA CON LA PLATAFORMA FALCON

Conecta los puntos
La estrecha integración con otros módulos de Falcon significa que usted puede alternar rápidamente entre información sobre vulnerabilidades, detalles sobre incidentes y actividades de endpoints, no solo en tiempo real, sino también retrospectivamente.

Previene durante el parcheo
La plataforma Falcon mitiga el riesgo de vulnerabilidades que no pueden ser parcheadas rápidamente, al prevenir y detectar intentos de exploits, así como actividades posteriores a una explotación. Esto le permite ganar un tiempo valioso para parchear sus sistemas contra ataques futuros.

SIN ESCANEOS O AGENTES NUEVOS

Elimina el escaneo
Falcon Spotlight utiliza el agente Falcon para monitorear continuamente el estado de vulnerabilidad de los endpoints y transmitir datos a la nube, eliminando la necesidad de realizar escaneos programados, al mismo tiempo que brinda una visibilidad completa sobre las vulnerabilidades.

Visibilidad en todas partes
Spotlight monitorea todos los endpoints por medio del sensor Falcon, tanto los que están dentro o fuera de la red, los que son on-premise, off-premise o en la nube, así como los físicos y virtuales.

Cero impacto en el desempeño
La gestión de vulnerabilidades no implica escaneos, siendo que éstas son identificadas en la nube, sin ningún impacto adicional en los endpoints o en la red.

ACCESO SIN FRICCIONES A DATOS SOBRE VULNERABILIDADES

Paneles y búsquedas en tiempo real
Falcon Spotlight hace que los datos estén disponibles fácilmente para los analistas de seguridad a través de una serie de paneles intuitivos y búsquedas en tiempo real. Las soluciones tradicionales bloquean información crucial en silos e informes de miles de páginas. Spotlight habilita esta información en tiempo real - cuando y donde se necesite.

API para integraciones personalizadas
La sólida API del Falcon Spotlight les permite a las organizaciones extraer datos sobre vulnerabilidades e integrarlos a sus propios flujos de trabajo de remediación automatizados.

EN LA NUBE

Fácil implementación
Como parte de la plataforma Falcon, el Falcon Spotlight no requiere la instalación de agentes adicionales ni de infraestructura o consolas de administración, haciendo que la implementación sea más fácil y eficiente.

Operando de forma inmediata
El Falcon Spotlight puede ser implementado de manera inmediata para una relación valor-tiempo incomparable. Tan pronto termina su instalación, éste comienza a funcionar, monitoreando e identificando vulnerabilidades en toda su organización, sin necesidad de reinicios, registro de consultas, ensayos o configuraciones complejas.

Una protección continua, basada en la nube
El Falcon Spotlight aprovecha la arquitectura nativa de la nube de CrowdStrike para darles a los equipos de seguridad el poder para proteger los sistemas - independientemente de si dichos sistemas son on-premise, están fuera de la red o en un entorno en la nube.

SEGURIDAD PREVENTIVA Y MÁS

La seguridad empieza destacando sus puntos de vulnerabilidad con el fin de que usted pueda cubrir sus vacíos de seguridad y prepararse lo mejor posible para enfrentar las amenazas. Falcon Spotlight ha sido diseñado para brindar la visibilidad e informaciones prácticas que los equipos de seguridad y TI necesitan para enfrentar las amenazas de manera exitosa.

SOBRE CROWDSTRIKE

CrowdStrike® Inc (Nasdaq: CRWD), un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints, dentro o fuera de la red. Alimentada por la tecnología patentada CrowdStrike Threat Graph™, la plataforma Falcon de CrowdStrike correlaciona más de dos billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.

© 2019 CrowdStrike, Inc.
Todos los derechos reservados.

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: CUMPLIMIENTO DE NORMAS DE SEGURIDAD INDUSTRIAL Y SALUD EN EL TRABAJO – CONTRATO NO. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **Unión Temporal UT273COGFM H&Y 2025**, en calidad de **Contratista**, manifiesta formalmente su compromiso de **garantizar la correcta prestación del Servicio de Suscripción Plataforma Protección de Datos – Lote No. 3**, conforme a los términos, condiciones y **acuerdos de nivel de servicio (ANS)** establecidos.
Durante la ejecución del contrato, el contratista dio estricto cumplimiento a las **normas de seguridad industrial y salud en el trabajo**, garantizando que todas las actividades desarrolladas se realizaran bajo **condiciones seguras y controladas**.

Se veló por la **integridad física del personal técnico y operativo**, mediante la aplicación de los protocolos establecidos en el **Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)**, el **uso adecuado de elementos de protección personal (EPP)** y la **implementación de medidas preventivas** para minimizar los riesgos laborales.

Asimismo, se aseguró el **cumplimiento de los lineamientos de seguridad** establecidos por la entidad contratante, manteniendo un **ambiente laboral seguro** durante las fases de transporte, instalación, configuración y pruebas de los equipos.

En consecuencia, la **Unión Temporal UT273COGFM H&Y 2025** acredita el **cumplimiento de las obligaciones en materia de seguridad industrial y salud en el trabajo**, conforme a la normatividad aplicable y a los compromisos contractuales adquiridos.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Next-Gen SIEM

Stop breaches by harnessing the speed and intelligence of the world's leading AI-native security platform

Legacy SIEMs can't keep pace with adversaries

Legacy SIEMs have failed the SOC. Excruciatingly slow, complex and costly, they were designed for an age that's long since passed, when data volumes and adversary speed were a fraction of today's.

Legacy SIEMs force security teams to spend more time setting up and maintaining log sources and rules rather than stopping breaches. SOC analysts have no choice but to waste endless hours manually triaging a massive volume of alerts and pivoting from console to console to uncover root cause, with agonizingly slow searches delaying investigations and increasing dwell times.

Soaring SIEM costs compound these risks by preventing teams from logging and retaining all of their data, causing blind spots and missed attacks. It's time for a new approach to security operations.

Pioneering the future of the AI-native SOC

CrowdStrike Falcon® Next-Gen SIEM revolutionizes threat detection, investigation and response by bringing together unmatched security depth and breadth in one unified platform to stop breaches. Falcon Next-Gen SIEM extends the industry's most dominant EDR, threat intelligence and expert services to all data sources for complete visibility and protection. Built from the ground up around a modern security analyst experience, it amplifies the speed and efficiency of incident response, so you can swiftly root out adversaries while slashing SOC costs.

Your team can detect and respond faster than you ever thought possible with real-time alerts, live dashboards and world-class intelligence. Your threat hunters can scour petabytes of data up to 150x times faster than legacy SIEMs with index-free search. Analyst-assist technologies transform all of your team members into experts by automating manual investigation steps and giving them a full picture of attacks with rich context. What took eight hours now takes eight minutes — and years of human expertise will help power every decision your team makes.

Key benefits

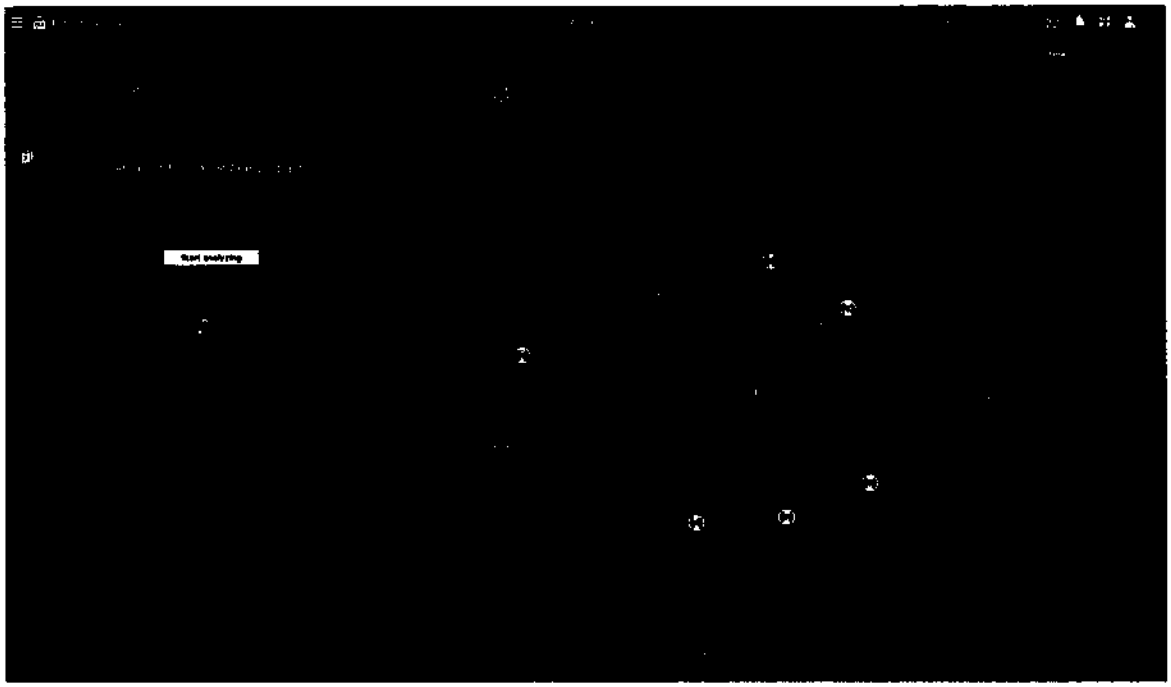
Detect threats in real time with AI powered analytics and correlation rules

Uplevel your analysts with world-class intelligence and Charlotte AI, the engine powering CrowdStrike's portfolio of generative AI capabilities

Reduce mean time to respond and say goodbye to tedious tasks with workflow automation

Coordinate response across your infrastructure and drive any endpoint remediation action through tight integration with the Falcon agent

Slash SOC costs by consolidating tools, streamlining operations and reducing capex compared to legacy SIEMs



Swiftly analyze incidents using XDR AI Investigator in Falcon Next-Gen SIEM

Falcon Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale platform that gives you unprecedented visibility across your entire digital estate. The lightweight Falcon agent simplifies data collection across endpoints and workloads, while an expanding set of data connectors harnesses the potential of all of your security tools and data.

Superior outcomes at a fraction of the cost of legacy SIEMs

With Falcon Next-Gen SIEM, you can safeguard your business with industry-leading, comprehensive security from the company that understands adversaries better than anyone. You can rest easy knowing experts from the world's top managed detection and response (MDR) provider are working round-the-clock for you. And for the first time ever, your team can leverage one unified data platform to hunt down and eliminate threats and address the compliance obligations and security challenges you face.

Key capabilities

Immediate time-to-value with simplified data onboarding and high-fidelity detections:

- **Out-of-the-box integrations to unlock the power of your security ecosystem:** Leverage a growing set of native data connectors, the CrowdStream observability pipeline and the Falcon Log Collector to easily collect data from any source, so you can spend more time fighting threats and less time onboarding data.
- **The key data you need — built in:** Get instant, native visibility from a unified, lightweight agent for endpoints, identities, cloud workloads and data protection. Break down silos and eliminate duplicate data stores by consolidating all threat detection, investigation and response in one high-performance platform.
- **Leading AI-powered detections, extended to all data sources:** Find the most sophisticated adversaries across all data sources with detections powered by the same advanced AI and behavior analysis as CrowdStrike's industry-leading endpoint detection and response (EDR).

Lightning-fast analysis with AI-led investigations:

- **Complete context for rapid, informed decisions:** Instantly understand an adversary's entire attack path across any data source with an elegant visual graph that unifies all threat context with user risk, vulnerabilities and asset relationships.
- **AI-native analyst-assist features:** Transform the investigative experience with AI-generated incidents that stitch together all related alerts, context and industry-leading threat intelligence with a plain-language summary of the adversary's actions.
- **Charlotte AI, the ultimate force-multiplier:** Ask any question to streamline investigations leveraging the power of high-fidelity data and generative AI. Users of all skill levels can elevate their ability to stop breaches with the optional Charlotte AI module.

Coordinated response to eliminate threats anywhere in your environment:

- **Fast resolution with fully integrated response:** Speed up investigation and response with leading threat intelligence and automation on your side. More than 125 workflow actions let you fully eradicate threats and free up your team to focus on higher-order operations.
- **Native SOAR capabilities to supercharge productivity:** Instantly stop adversaries with workflow automation, powered by CrowdStrike Falcon® Fusion, to orchestrate remediation actions across the CrowdStrike platform and third-party tools — all from one, unified console.
- **Tight integration with the Falcon agent to drive any endpoint action:** Leverage powerful Falcon platform features, such as Falcon Real Time Response, to contain fast-moving attacks and limit adversary lateral movement using pre-built commands and extensible scripts.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

See Next-Gen SIEM in Action →

This document includes forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actua results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

© 2024 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE

CrowdStrike Products

Data Sheet

Falcon Identity Threat Protection

Prevent breaches with unified identity threat detection and response (ITDR)

CrowdStrike Falcon® Identity Threat Protection, the CrowdStrike Falcon® identity threat detection and response (ITDR) module, detects and stops identity-based breaches in real time. The Falcon platform leverages a single, lightweight sensor that provides attack correlation across endpoints, identity, workloads and data. Falcon Identity Threat Protection extends protection into legacy and unmanaged systems, providing better MITRE ATT&CK® coverage and frictionless, risk-based conditional access.

Key product capabilities

Segment

Gain granular and continuous insights into every account and activity to highlight identity security gaps across identity stores, and empower your identity and access management (IAM) and security teams to better evaluate identities and the risks associated with them.

Continuous multi-directory visibility: Get deeper visibility into the scope and the impact of access privileges for identities across Microsoft Active Directory (AD) and Entra ID.

Auto-classification of all accounts: Automatically classify identities into hybrid (identities that are on-premises and cloud AD) and cloud-only (identities that reside only on Entra ID), and segment accounts into human, service, shared accounts and privileged accounts.

Customizable AD security posture overview: Analyze user risk and behavior changes over time, like increase in account lockouts, high-risk endpoints and duplicate/compromised passwords to get an overview of the attack surface of the organization.

Key benefits

- Realize value from Day One by gaining unified visibility and control of access to applications, resources and identity stores in hybrid environments
- Reduce mean time to detect and respond, and improve SOC analysts' efficiency and response times by collating all connected anomalies and alerts into incidents
- Improve alert fidelity and reduce noise by recognizing and auto-resolving genuine access incidents through identity verification
- Enforce consistent risk-based policies to enable Zero Trust architecture with zero-trust on actions inside block, allow, audit and step-up using multi-factor authentication (MFA)
- Save log storage costs by storing only relevant authentication logs
- Increase ROI from your MFA investment by extending it to legacy applications and tools

Automate

Enable real-time identity threat detection and protection without time-consuming log processing. Eliminate risky guesswork and prioritize authentication tasks based on over 100 behavior analytics and risk factors for every account.

Hybrid identity store protection: Continuously assess the directory configuration, like Group Policy Objects (GPO), LDAP configurations and risky implementation of protocols like RDP to DC and SMB to DC. Analyze every account from on-premises to hybrid identity stores. Inspect live authentication traffic, including encrypted protocols (e.g., LDAP/S).

Real-time threat detection: Continuously assess identity events and automatically associate them with threats and malicious intent, in real time, without ingesting logs with Falcon Identity Threat Protection's out-of-the-box machine-learning-powered detection rules. With advanced analytics and patented machine learning, uncover reconnaissance (e.g., LDAP, BloodHound, SharpHound, credential compromise attacks), lateral movement (e.g., RDP, pass-the-hash (PtH), Mimikatz tool, unusual endpoint usage, unusual service logins, etc.), and persistence (e.g., Golden Ticket attack, privilege escalation, etc.).

Intuitive threat hunting: Investigate faster with unified domain access into detailed activities of every account across hybrid identity stores without the need for complex, string-based queries. Choose from a list of predefined search criteria, including authentication events, use of unencrypted protocols, user roles, IP reputation, risk scores and many more. Safely lure adversaries with honeytoken accounts and get dedicated insights into their attack paths. If required, create and save your own search criteria to proactively sift through raw events and email them as periodic reports.

Comprehensive API coverage: Extend the Falcon platform's risk score and high-fidelity information to other apps (e.g., AD FS, SSO, IT systems and over 50 integrations) with minimal effort using API-based connectors.

Verify

Secure employee or contractor access to applications, tools and resources with a zero-friction user experience. Ensure consistent login experience for genuine users, but automatically step up authentication when risk scores increase.

Zero-friction identity verification with flexible policies: Define and enforce access policies with simple rules with Falcon Identity Threat Protection adaptive analysis, eliminating the need to write complex static conditions for every user. The policies are based on authentication patterns, behavior baselines, individual user risk score and device risk score (via API integration) to verify identities using MFA. This robust methodology secures access to identity stores and applications, with improved user experience — e.g., identity verification is triggered only when the risk increases or if there's a deviation from normal behavior.

Improved security posture with extended MFA: Extend identity verification/MFA to any resource or application, including legacy/proprietary systems and tools that traditionally could not be integrated with MFA — for example, desktops that are not covered by cloud-based MFA solutions, and tools like PowerShell and protocols like RDP over NTLM — to reduce the attack surface.

Auto-resolve security incidents: With the platform's customizable enforcement policies, resolve standard incidents that the user approves using identity verification methods (2FA/MFA), so that your security analysts can focus on critical security incidents. Additionally, resolve these incidents with effortless API integrations into SOAR, SIEM and ticketing platforms.

Frictionless AD security

- **Multi-directory identity layer support:** Falcon Identity Threat Protection natively supports Microsoft AD and Entra ID, provides only the weakest link in your cyber defenses and also integrates with SSO and federation solutions like Okta, AD FS and PingFederate.
- **Broad MFA support:** Falcon Identity Threat Protection supports multiple MFA solutions, including Okta, Duo, ID Pingid, RSA CAS, Beyond and more.
- **Extended protocol coverage:** Falcon Identity Threat Protection provides granular visibility and control over encrypted protocols like NTLM and LDAPS, which are difficult to detect with traditional tools like SIEM and UEBA.
- **Extensive API coverage:** Falcon Identity Threat Protection enables over 50 integrations with API based connectors, providing easy integration with identity as a service (IDaaS)/SSO, SIEM, SOAR, ticketing and asset management solutions.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

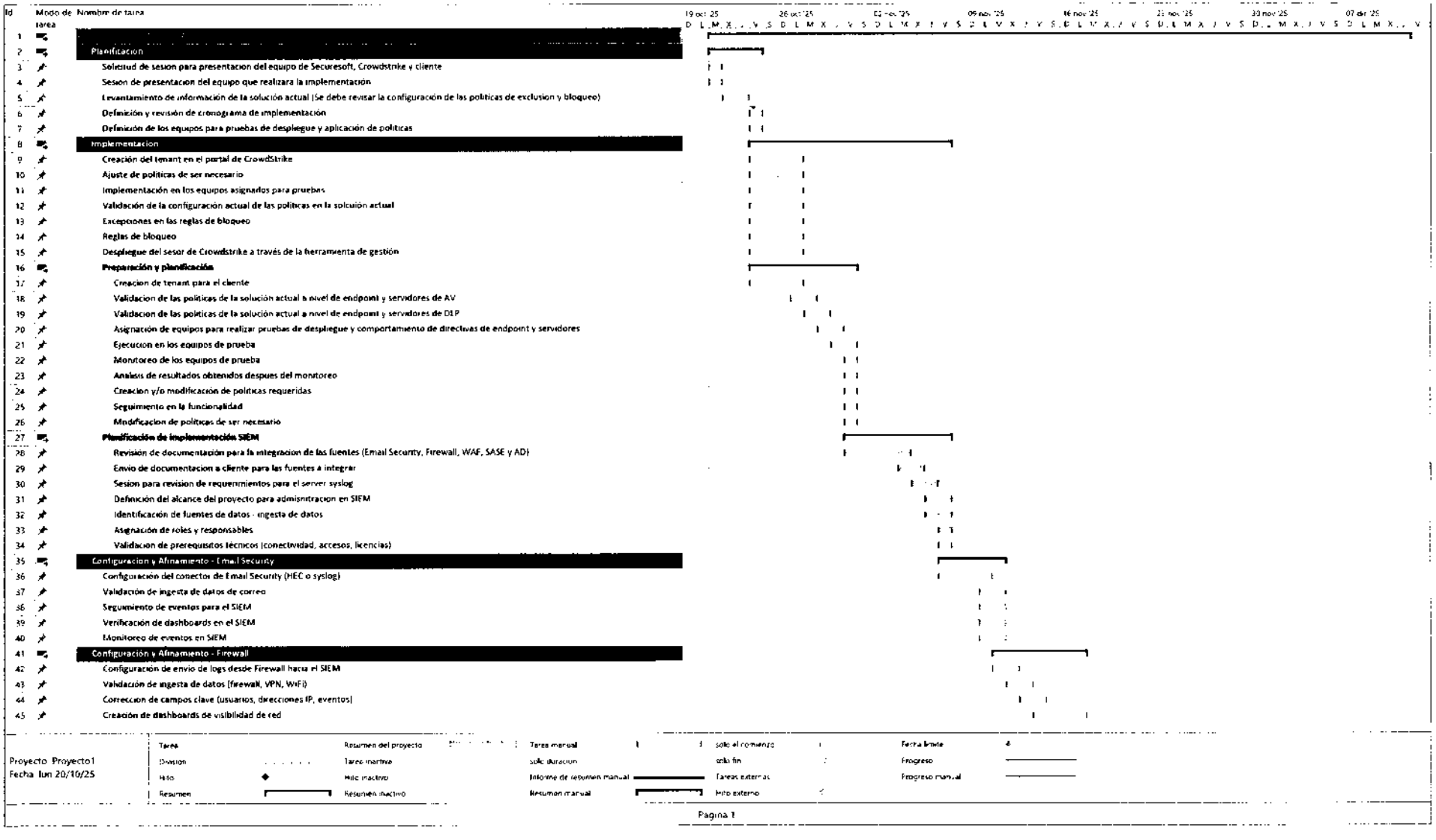
Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

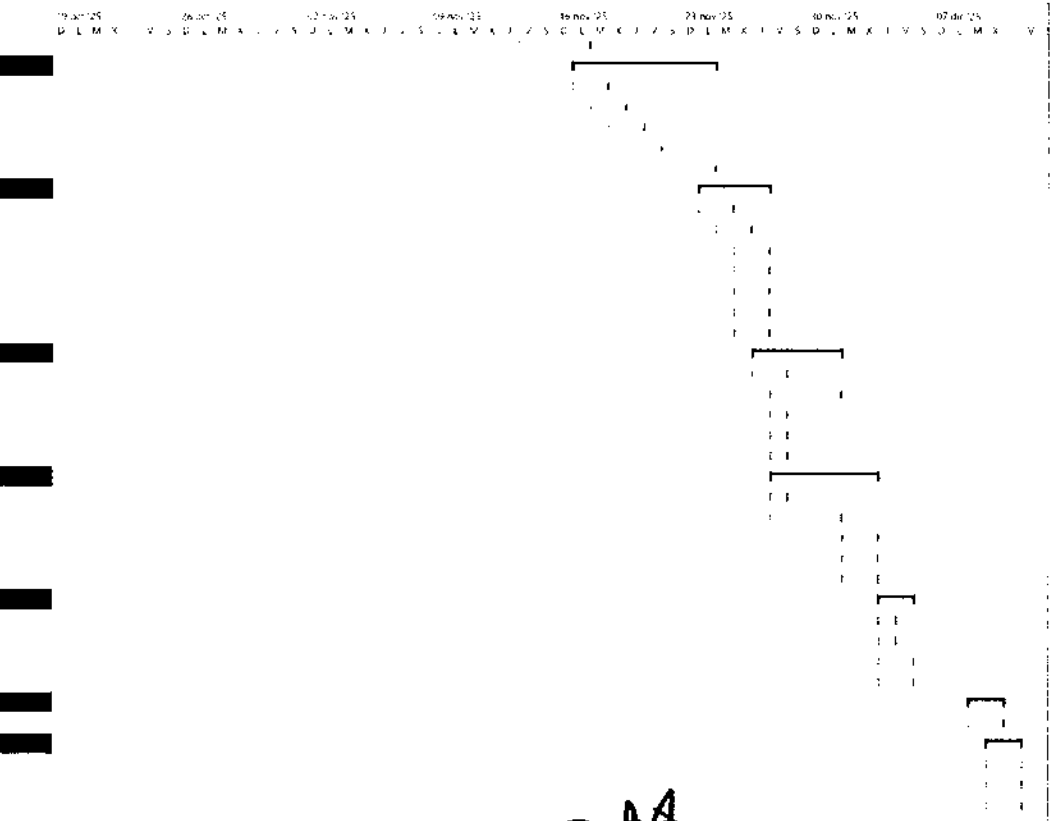
CrowdStrike: We stop breaches.

Start a Free Trial →

© 2024 CrowdStrike, Inc.


Id
Modo de tarea
Nombre de tarea
19 oct '25
26 oct '25
02 nov '25
09 nov '25
16 nov '25
23 nov '25
30 nov '25
07 dic '25
1
2 Planificacion
3 Solicitud de sesion para presentacion del equipo de Securesoft, Crowdstrike y cliente
4 Sesion de presentacion del equipo que realizara la implementación
5 Levantamiento de información de la solución actual (Se debe revisar la configuración de las politicas de exclusion y bloqueo)
6 Definición y revisión de cronograma de implementación
7 Definición de los equipos para pruebas de despliegue y aplicación de politicas
8 Implementacion
9 Creación del tenant en el portal de CrowdStrike
10 Ajuste de politicas de ser necesario
11 Implementación en los equipos asignados para pruebas
12 Validación de la configuración actual de las politicas en la solución actual
13 Excepciones en las reglas de bloqueo
14 Reglas de bloqueo
15 Despliegue del sesor de Crowdstrike a través de la herramienta de gestión
16 Preparación y planificación
17 Creacion de tenant para el cliente
18 Validacion de las politicas de la solución actual a nivel de endpoint y servidores de AV
19 Validacion de las politicas de la solución actual a nivel de endpoint y servidores de DLP
20 Asignación de equipos para realizar pruebas de despliegue y comportamiento de directivas de endpoint y servidores
21 Ejecucion en los equipos de prueba
22 Monitoreo de los equipos de prueba
23 Analisis de resultados obtenidos despues del monitoreo
24 Creacion y/o modificación de politicas requeridas
25 Seguimiento en la funcionalidad
26 Modificacion de politicas de ser necesario
27 Planificación de implementación SIEM
28 Revisión de documentación para la integracion de las fuentes (Email Security, Firewall, WAF, SASE y AD)
29 Envio de documentacion a cliente para las fuentes a integrar
30 Sesion para revision de requerimientos para el server syslog
31 Definición del alcance del proyecto para adminsitracion en SIEM
32 Identificación de fuentes de datos - ingesta de datos
33 Asignación de roles y responsables
34 Validacion de prerequisitos técnicos (conectividad, accesos, licencias)
35 Configuracion y Afinamiento - Email Security
36 Configuración del conector de Email Security (HEC o syslog)
37 Validación de ingesta de datos de correo
38 Seguimiento de eventos para el SIEM
39 Verificación de dashboards en el SIEM
40 Monitoreo de eventos en SIEM
41 Configuración y Afinamiento - Firewall
42 Configuración de envio de logs desde Firewall hacia el SIEM
43 Validación de ingesta de datos (firewall, VPN, WiFi)
44 Correccion de campos clave (usuarios, direcciones IP, eventos)
45 Creación de dashboards de visibilidad de red
Proyecto: Proyecto1
Fecha: lun 20/10/25
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
Sólo duración
Informe de resumen manual
Resumen manual
Sólo el comienzo
Sólo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 1

Id	Modo de tarea	Nombre de tarea
46		Monitoreo de eventos en SIEM
47		**Configuracion y Afinamiento - WAF**
48		Configuración del conector WAF
49		Validación de ingesta de datos
50		Seguimiento de eventos para el SIEM
51		Verificacion de dashboards en el SIEM
52		Monitoreo de eventos en SIEM
53		**Configuracion y Afinamiento - SASE**
54		Configuracion de conector SASE
55		Validación de logs de navegacion
56		Ajuste de parsing y categorizacion en SIEM
57		Creacion de alertas para trafico sospechoso
58		Seguimiento de eventos para el SIEM
59		Verificación de dashboards en el SIEM
60		Monitoreo de eventos en SIEM
61		**Configuracion y Afinamiento - AD**
62		Configuracion del conector AD
63		Validacion de ingesta de datos
64		Seguimiento de eventos para el SIEM
65		Verificación de dashboards en el SIEM
66		Monitoreo de eventos en SIEM
67		**Pruebas y validacion**
68		Simulación de incidentes de seguridad (correo, navegación, red)
69		Validación de correlación entre las fuentes
70		Ajuste de alertas para reducir falsos positivos
71		Validacion con SOC y proceso de alertamiento
72		Documentación de resultados de las pruebas
73		**Dashboards iniciales y alertas**
74		Creación de dashboards para informes y analistas
75		Configuración de alertas en tiempo real
76		Validacion de reportes automáticos para cliente
77		Desarrollo casos de uso
78		**Capacitacion**
79		Capacitacion del equipo
80		**Cierre**
81		Elaboración de documentación de implementación
82		Entrega de documentacion de cierre de implementación del proyecto
83		Reunión de cierre de implementación del proyecto



JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

JOSE FRANCISCO LOMBANA CARDONA
C. C.14.395.966
Supervisor Contrato No. 259/2025

Proyecto: Proyecto1
Fecha: lun 20/10/25

Tarea | División | Hito | Resumen | Resumen del proyecto | Tarea inactiva | Hito inactivo | Resumen inactivo | Tarea manual | Solo duración | Informe de resumen manual | Resumen manual | Solo el comienzo | Solo fin | Tareas externas | Hito externo | Fecha límite | Progreso | Progreso manual

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE EJECUCIÓN A TODO COSTO Y ALCANCE DEL SERVICIO

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025, la UT 273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente que la ejecución del contrato se realizará **a todo costo**, entendiendo por ello que serán de su exclusiva responsabilidad todos los gastos, recursos, actividades, personal, herramientas, licencias, materiales y demás elementos necesarios para la correcta prestación del servicio.
El Contratista se compromete a:

1. **Prestar el servicio objeto del contrato** incluyendo, de manera integral, las actividades de **instalación, configuración, implementación y puesta en marcha** de la solución contratada.
2. **Realizar las pruebas de funcionalidad necesarias** para verificar el correcto desempeño de la solución, dejando evidencia de las **pruebas exitosas de funcionalidad** y asegurando que el servicio quede plenamente operativo conforme a las especificaciones técnicas y a los requerimientos del supervisor del contrato.
3. Asumir todos los costos y recursos requeridos para atender las obligaciones aquí descritas, sin que ello genere costos adicionales para la Entidad Contratante, salvo los expresamente pactados en el contrato principal.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

COMPROMISO CONFIDENCIALIDAD

SERA DILIGENCIADO AL MOMENTO DE SUSCRIPCIÓN DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mi propio nombre y de los funcionarios o asesores que se vinculen a la misma para efectos de ejecución del presente contrato, asume el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que el **MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA** adelantó el proceso de selección del Contrato de No. 259 , cuyo objeto es PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO.

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares del Ministerio a los cuales tenga acceso.

CUARTA: Que acepto y permito al Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, utilizar de manera responsable y de acuerdo con la política de protección de datos personales, la información que he proporcionado, para lo cual garantizó que son exactos, por lo que, en caso de ser modificados, comunicaré al Ministerio, para que sean rectificados y/o cancelados según proceda.

QUINTA: **Que, por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:**

CLÁUSULA PRIMERA. COMPROMISO ASUMIDO POR EL CONTRATISTA: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

EL CONTRATISTA se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.

b) No permitir que terceros obtengan información relacionada con el literal anterior.

c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

e) No dar, ofrecer dadivas, regalos, beneficios, comisiones, promesa remuneratoria, directa o indirectamente; tanto en el ministerio o fuera de él, a cambio de obtener beneficios ilegales en la ejecución de sus obligaciones contractuales.

f) Fomentar el reporte de conductos, hechos que puedan llegar a configurasen en prácticas de soborno, corrupción, con fundamento en la buena fe o en una sospecha razonable.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: EL CONTRATISTA asume a través de la suscripción del presente compromiso, las consecuencias que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente EL CONTRATISTA que toda la información que se produzca en la ejecución del contrato será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá, D.C. a los (09) días del mes de julio del dos mil veinticuatro (2025).

EL CONTRATISTA

Nombre: JESÚS ALBERTO FRANCO ACOSTA
C.E. No. 582410

Este anexo hará parte integral del contrato respectivo.

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: Entrega de Ponderables – Contrato No. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del Contrato No. 259COGFM DIADF 2025, la Unión Temporal UT273COGFM H&Y 2025, en calidad de Contratista, manifiesta formalmente su compromiso de garantizar la correcta prestación del Servicio de Suscripción Plataforma Protección de Datos – Lote No. 3.

En atención al requerimiento de entrega de los ponderables correspondientes, se informa que se ha realizado la entrega efectiva de los compromisos establecidos, conforme se detalla a continuación:

1	**El contratista ofrece sin costo adicional:** Transferencia de conocimiento de la solución de protección de datos ofertada con certificación de Voucher para cuatro (4) funcionarios del Comando General de las Fuerzas Militares – CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM	1	$20,749,691.32	20,749,691.32

De esta manera, la Unión Temporal UT273COGFM H&Y 2025 ratifica el cumplimiento de los compromisos adquiridos y reitera su disposición para atender cualquier requerimiento adicional que contribuya al correcto desarrollo del contrato

Yeapdata®

Heimcore

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Carlos Giovani Diaz Rueda

De: Alejandro Gonzalez <alejandro.gonzalez@crowdstrike.com>
Enviado el: miércoles, 10 de diciembre de 2025 09:42 a. m.
Para: Carlos Giovani Diaz Rueda
CC: Andres Rodrigo Rodriguez Castañeda
Asunto: Re: [External] Transferencia de conocimiento - Voucher para cuatro (04) funcionarios - Crowdstrike

Hola

La información completa

Thanks for reaching out.

Please find your account's exam voucher codes below. Additionally, please ensure they are used to both schedule and attend exams occurring prior to the expiration date listed.

Voucher Code	Voucher Expiration Date	Voucher Status
CSPU382B5D0A	10/30/2026	Available
CSPU39223D4E	10/30/2026	Available
CSPU39293A1D	10/30/2026	Available
CSPU39989D93	10/30/2026	Available

Please follow these steps when you're ready to take your CrowdStrike Certification Exam:

1. Sign in to CrowdStrike University
    - If this is your first time taking a CrowdStrike certification exam, find your CrowdStrike University ID on your profile page and make note of it – you will need to input this when you create your exam taker account with Pearson VUE
2. Select Prepare and Get Certified from the CrowdStrike University homepage
3. Select Schedule your certification exam, which will redirect you to the Pearson VUE/CrowdStrike website where you can create your exam taker account and register for your exam
    - If you encounter any scheduling issues online, you may call Pearson VUE at 866-980-0413 to schedule your exam
4. When creating your exam taker account profile, be sure to add your CrowdStrike University ID

Yeapdata®

Heimcore

4. Garantía de soporte

Como parte de la garantía técnica asociada a la Suscripción de Protección de Datos, se establece que:

- El Contratista deberá **garantizar el normal funcionamiento de la solución** después de la implementación y puesta en marcha.
  En caso de presentarse fallas atribuibles a la implementación, configuración o parametrización, el Contratista deberá **asumir los gastos** necesarios (configuraciones adicionales, horas de ingenieros, visitas a sitio, entre otros) que se generen hasta restablecer el funcionamiento de la solución, en un tiempo no mayor a **veinticuatro (24) horas**.
- El soporte deberá estar disponible los **365 días del año**, en horario **7x24** (7 días a la semana, 24 horas al día).
- El servicio de soporte deberá ser atendido de manera **inmediata** a través de:
  - Una **línea telefónica gratuita**,
  - Servicio de **correo electrónico**, y/o
  - Atención **remota**,
  -

Conforme a los niveles de servicio acordados.

- En caso de que, en un lapso de **cuatro (4) horas** después de haber sido reportado el incidente, **no se haya dado solución** al mismo, el Contratista deberá **enviar personal técnico especializado a sitio** en un tiempo máximo de **dos (2) horas** adicionales, manteniendo la atención hasta el restablecimiento total de la suscripción y de la operación normal del servicio de protección de datos.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

FALCON SPOTLIGHT

Un nuevo enfoque para la gestión de vulnerabilidades

La solución más rápida y sencilla para reducir el riesgo y la exposición, cubrir los vacíos de seguridad y estar mejor preparado para responder a los ataques

FALCON SPOTLIGHT

GESTIÓN DE VULNERABILIDADES INSTANTÁNEA Y SIN ESCANEOS

CrowdStrike® Falcon Spotlight™ les ofrece a los equipos de seguridad una evaluación en tiempo real, y siempre actualizada, de la exposición a vulnerabilidades de sus endpoints. La integración nativa del Falcon Spotlight en la plataforma Falcon® de CrowdStrike les permite a los clientes gestionar las vulnerabilidades dentro de un marco completo de protección de endpoints. Falcon Spotlight añade preparación y prontitud a la inigualable prevención, detección y respuesta de la plataforma Falcon, lo que resulta en una postura de seguridad más fuerte y una protección contra las brechas incomparable.

- **Protección Integrada:** Spotlight es un componente clave de la plataforma integral y unificada de protección para endpoints de CrowdStrike. Con Spotlight y la plataforma Falcon, usted no solo puede ver sus vacíos de seguridad, sino, también, a cuáles de éstos les están apuntando sus adversarios. Esto le permite armarse con la protección proactiva que se necesita para bloquear ataques avanzados.
- **Visibilidad Integral:** Spotlight no requiere escaneos ni agentes nuevos para su implementación y manejo - solo tiene que prenderlo y empezar a ver los resultados. Spotlight le brinda visibilidad en toda su empresa, independientemente de si los endpoints son físicos o virtuales, on u off-premise, o móviles. Usted recibe una visibilidad incomparable sobre las vulnerabilidades en todos sus negocios distribuidos, sin afectaciones.
- **Sencillo:** Spotlight ofrece, continuamente, una información que está siempre actualizada, poniéndola en manos de los analistas de seguridad. Esto le ayuda a mejorar el tiempo de respuesta, reduciendo el esfuerzo que implica comprender su postura de seguridad y volverse más proactivo.
- **Cero impacto:** la arquitectura nativa de la nube de CrowdStrike permite tener una visibilidad constante sobre las vulnerabilidades de los endpoints, sin necesidad de realizar complicados escaneos de red o host que demanden un gran uso de recursos.

PRINCIPALES BENEFICIOS

Falcon Spotlight ofrece una gestión de vulnerabilidades sin escaneos. Construido sobre la plataforma Falcon, éste ofrece evaluaciones oportunas y sin impacto de la postura de seguridad de endpoints, así como acceso bajo demanda a los resultados. Esto les permite a los equipos de seguridad reducir el riesgo y tomar mejores decisiones de manera más rápida.

Brinda una protección integral que cierra las brechas entre la gestión de vulnerabilidades y la prevención de amenazas

Ofrece una implementación fácil y nativa de la nube que no requiere agentes adicionales o nueva infraestructura

Ofrece información oportuna y actualizada bajo demanda

Provee evaluaciones sin impacto y sin escaneos

PRINCIPALES CAPACIDADES DEL PRODUCTO

Falcon Spotlight resuelve los desafíos que afectan a las soluciones tradicionales de gestión de vulnerabilidades, ofreciendo los siguientes beneficios:

INTEGRACIÓN PERFECTA CON LA PLATAFORMA FALCON

Conecta los puntos
La estrecha integración con otros módulos de Falcon significa que usted puede alternar rápidamente entre información sobre vulnerabilidades, detalles sobre incidentes y actividades de endpoints, no solo en tiempo real, sino también retrospectivamente.

Previene durante el parcheo
La plataforma Falcon mitiga el riesgo de vulnerabilidades que no pueden ser parcheadas rápidamente, al prevenir y detectar intentos de exploits, así como actividades posteriores a una explotación. Esto le permite ganar un tiempo valioso para parchear sus sistemas contra ataques futuros.

SIN ESCANEOS O AGENTES NUEVOS

Elimina el escaneo
Falcon Spotlight utiliza el agente Falcon para monitorear continuamente el estado de vulnerabilidad de los endpoints y transmitir datos a la nube, eliminando la necesidad de realizar escaneos programados, al mismo tiempo que brinda una visibilidad completa sobre las vulnerabilidades.

Visibilidad en todas partes
Spotlight monitorea todos los endpoints por medio del sensor Falcon, tanto los que están dentro o fuera de la red, los que son on-premise, off-premise o en la nube, así como los físicos y virtuales.

Cero impacto en el desempeño
La gestión de vulnerabilidades no implica escaneos, siendo que éstas son identificadas en la nube, sin ningún impacto adicional en los endpoints o en la red.

ACCESO SIN FRICCIONES A DATOS SOBRE VULNERABILIDADES

Paneles y búsquedas en tiempo real
Falcon Spotlight hace que los datos estén disponibles fácilmente para los analistas de seguridad a través de una serie de paneles intuitivos y búsquedas en tiempo real. Las soluciones tradicionales bloquean información crucial en silos e informes de miles de páginas. Spotlight habilita esta información en tiempo real - cuando y donde se necesite.

API para integraciones personalizadas
La sólida API del Falcon Spotlight les permite a las organizaciones extraer datos sobre vulnerabilidades e integrarlos a sus propios flujos de trabajo de remediación automatizados.

EN LA NUBE

Fácil implementación
Como parte de la plataforma Falcon, el Falcon Spotlight no requiere la instalación de agentes adicionales ni de infraestructura o consolas de administración, haciendo que la implementación sea más fácil y eficiente.

Operando de forma inmediata
El Falcon Spotlight puede ser implementado de manera inmediata para una relación valor-tiempo incomparable. Tan pronto termina su instalación, éste comienza a funcionar, monitoreando o identificando vulnerabilidades en toda su organización, sin necesidad de reinicios, registro de consultas, ensayos o configuraciones complejas.

Una protección continua, basada en la nube
El Falcon Spotlight aprovecha la arquitectura nativa de la nube de CrowdStrike para darles a los equipos de seguridad el poder para proteger los sistemas - independientemente de si dichos sistemas son on-premise, están fuera de la red o en un entorno en la nube.

SEGURIDAD PREVENTIVA Y MÁS

La seguridad empieza destacando sus puntos de vulnerabilidad con el fin de que usted pueda cubrir sus vacíos de seguridad y prepararse lo mejor posible para enfrentar las amenazas. Falcon Spotlight ha sido diseñado para brindar la visibilidad e informaciones prácticas que los equipos de seguridad y TI necesitan para enfrentar las amenazas de manera exitosa.

SOBRE CROWDSTRIKE

CrowdStrike® Inc (Nasdaq: CRWD), un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints dentro o fuera de la red. Alimentada por la tecnología patentada CrowdStrike Threat Graph®, la plataforma Falcon de CrowdStrike correlaciona más de dos billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.

© 2019 CrowdStrike, Inc.
Todos los derechos reservados.

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: CUMPLIMIENTO DE NORMAS DE SEGURIDAD INDUSTRIAL Y SALUD EN EL TRABAJO – CONTRATO NO. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **Contrato No. 259COGFM DIADF 2025**, la **Unión Temporal UT273COGFM H&Y 2025**, en calidad de **Contratista**, manifiesta formalmente su compromiso de **garantizar la correcta prestación del Servicio de Suscripción Plataforma Protección de Datos – Lote No. 3**, conforme a los términos, condiciones y **acuerdos de nivel de servicio (ANS)** establecidos.
Durante la ejecución del contrato, el contratista dio estricto cumplimiento a las **normas de seguridad industrial y salud en el trabajo**, garantizando que todas las actividades desarrolladas se realizaran bajo **condiciones seguras y controladas**.

Se veló por la **integridad física del personal técnico y operativo**, mediante la aplicación de los protocolos establecidos en el **Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)**, el **uso adecuado de elementos de protección personal (EPP)** y la **implementación de medidas preventivas** para minimizar los riesgos laborales.

Asimismo, se aseguró el **cumplimiento de los lineamientos de seguridad** establecidos por la entidad contratante, manteniendo un **ambiente laboral seguro** durante las fases de transporte, instalación, configuración y pruebas de los equipos.

En consecuencia, la **Unión Temporal UT273COGFM H&Y 2025** acredita el **cumplimiento de las obligaciones en materia de seguridad industrial y salud en el trabajo**, conforme a la normatividad aplicable y a los compromisos contractuales adquiridos.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Next-Gen SIEM

Stop breaches by harnessing the speed and intelligence of the world's leading AI-native security platform

Legacy SIEMs can't keep pace with adversaries

Legacy SIEMs have failed the SOC. Excruciatingly slow, complex and costly, they were designed for an age that's long since passed, when data volumes and adversary speed were a fraction of today's.

Legacy SIEMs force security teams to spend more time setting up and maintaining log sources and rules rather than stopping breaches. SOC analysts have no choice but to waste endless hours manually triaging a massive volume of alerts and pivoting from console to console to uncover root cause, with agonizingly slow searches delaying investigations and increasing dwell times.

Soaring SIEM costs compound these risks by preventing teams from logging and retaining all of their data, causing blind spots and missed attacks. It's time for a new approach to security operations.

Pioneering the future of the AI-native SOC

CrowdStrike Falcon® Next-Gen SIEM revolutionizes threat detection, investigation and response by bringing together unmatched security depth and breadth in one unified platform to stop breaches. Falcon Next-Gen SIEM extends the industry's most dominant EDR, threat intelligence and expert services to all data sources for complete visibility and protection. Built from the ground up around a modern security analyst experience, it amplifies the speed and efficiency of incident response, so you can swiftly root out adversaries while slashing SOC costs.

Your team can detect and respond faster than you ever thought possible with real-time alerts, live dashboards and world-class intelligence. Your threat hunters can scour petabytes of data up to 150x times faster than legacy SIEMs with index-free search. Analyst-assist technologies transform all of your team members into experts by automating manual investigation steps and giving them a full picture of attacks with rich context. What took eight hours now takes eight minutes — and years of human expertise will help power every decision your team makes.

Key benefits

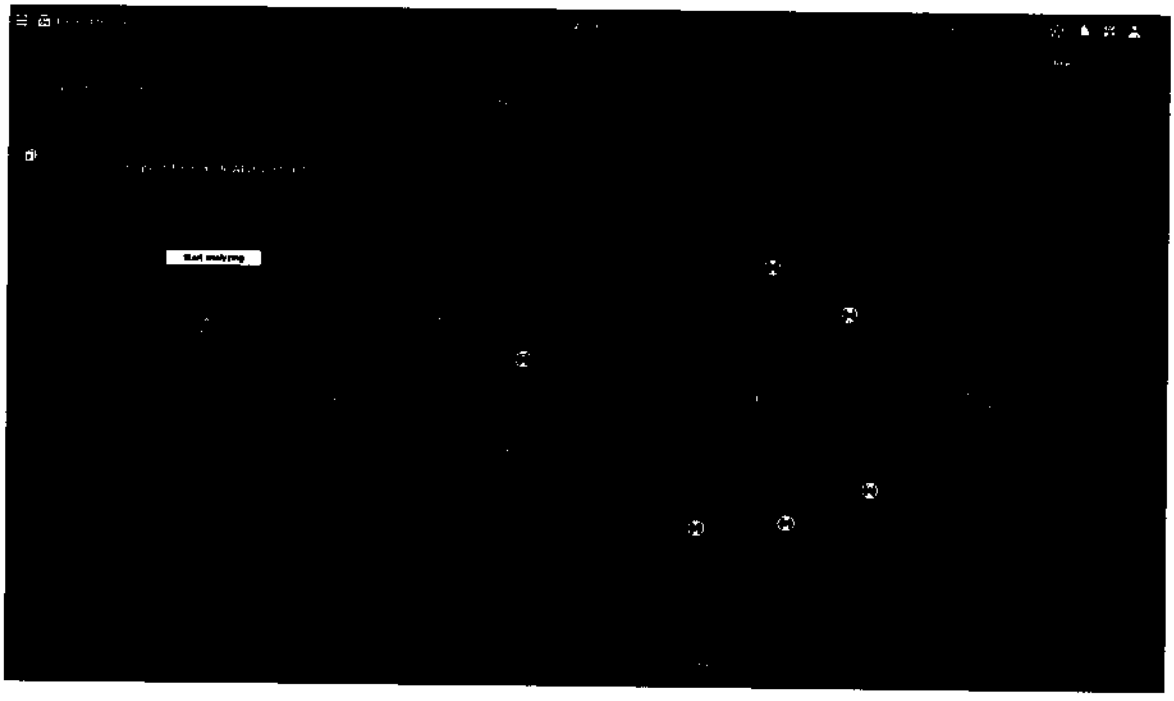
Detect threats in real time with AI powered analytics and correlation rules

Uplevel your analysts with world class intelligence and Charlotte AI, the engine powering CrowdStrike's portfolio of generative AI capabilities

Reduce mean time to respond and say goodbye to tedious tasks with workflow automation

Coordinate response across your infrastructure and drive any endpoint remediation action through tight integration with the Falcon agent

Slash SOC costs by consolidating tools, streamlining operations and reducing capex compared to legacy SIEMs



Swiftly analyze incidents using XDR AI Investigator in Falcon Next-Gen SIEM

Falcon Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale platform that gives you unprecedented visibility across your entire digital estate. The lightweight Falcon agent simplifies data collection across endpoints and workloads, while an expanding set of data connectors harnesses the potential of all of your security tools and data.

Superior outcomes at a fraction of the cost of legacy SIEMs

With Falcon Next-Gen SIEM, you can safeguard your business with industry-leading, comprehensive security from the company that understands adversaries better than anyone. You can rest easy knowing experts from the world's top managed detection and response (MDR) provider are working round-the-clock for you. And for the first time ever, your team can leverage one unified data platform to hunt down and eliminate threats and address the compliance obligations and security challenges you face.

Key capabilities

Immediate time-to-value with simplified data onboarding and high-fidelity detections:

- **Out-of-the-box integrations to unlock the power of your security ecosystem:** Leverage a growing set of native data connectors, the CrowdStream observability pipeline and the Falcon Log Collector to easily collect data from any source, so you can spend more time fighting threats and less time onboarding data.
- **The key data you need — built in:** Get instant, native visibility from a unified, lightweight agent for endpoints, identities, cloud workloads and data protection. Break down silos and eliminate duplicate data stores by consolidating all threat detection, investigation and response in one high-performance platform.
- **Leading AI-powered detections, extended to all data sources:** Find the most sophisticated adversaries across all data sources with detections powered by the same advanced AI and behavior analysis as CrowdStrike's industry-leading endpoint detection and response (EDR).

Lightning-fast analysis with AI-led investigations:

- **Complete context for rapid, informed decisions:** Instantly understand an adversary's entire attack path across any data source with an elegant visual graph that unifies all threat context with user risk, vulnerabilities and asset relationships.
- **AI-native analyst-assist features:** Transform the investigative experience with AI-generated incidents that stitch together all related alerts, context and industry-leading threat intelligence with a plain-language summary of the adversary's actions.
- **Charlotte AI, the ultimate force-multiplier:** Ask any question to streamline investigations leveraging the power of high-fidelity data and generative AI. Users of all skill levels can elevate their ability to stop breaches with the optional Charlotte AI module.

Coordinated response to eliminate threats anywhere in your environment:

- **Fast resolution with fully integrated response:** Speed up investigation and response with leading threat intelligence and automation on your side. More than 125 workflow actions let you fully eradicate threats and free up your team to focus on higher-order operations.
- **Native SOAR capabilities to supercharge productivity:** Instantly stop adversaries with workflow automation, powered by CrowdStrike Falcon® Fusion, to orchestrate remediation actions across the CrowdStrike platform and third-party tools — all from one, unified console.
- **Tight integration with the Falcon agent to drive any endpoint action:** Leverage powerful Falcon platform features, such as Falcon Real Time Response, to contain fast-moving attacks and limit adversary lateral movement using pre-built commands and extensible scripts.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

See Next-Gen SIEM in Action →

This document includes forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

© 2024 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Identity Threat Protection

Prevent breaches with unified identity threat detection and response (ITDR)

CrowdStrike Falcon® Identity Threat Protection, the CrowdStrike Falcon® identity threat detection and response (ITDR) module, detects and stops identity-based breaches in real time. The Falcon platform leverages a single, lightweight sensor that provides attack correlation across endpoints, identity, workloads and data. Falcon Identity Threat Protection extends protection into legacy and unmanaged systems, providing better MITRE ATT&CK® coverage and frictionless, risk-based conditional access.

Key product capabilities

Segment

Gain granular and continuous insights into every account and activity to highlight identity security gaps across identity stores, and empower your identity and access management (IAM) and security teams to better evaluate identities and the risks associated with them.

Continuous multi-directory visibility: Get deeper visibility into the scope and the impact of access privileges for identities across Microsoft Active Directory (AD) and Entra ID.

Auto-classification of all accounts: Automatically classify identities into hybrid (identities that are on-premises and cloud AD) and cloud-only (identities that reside only on Entra ID), and segment accounts into human, service, shared accounts and privileged accounts.

Customizable AD security posture overview: Analyze user risk and behavior changes over time, like increase in account lockouts, high-risk endpoints and duplicate/compromised passwords to get an overview of the attack surface of the organization.

Key benefits

- Realize value from Day One gain unified visibility and control of access to applications, resources and identity stores in hybrid environments
- Reduce mean time to detect and respond, and improve SOC analysts' efficiency and response times by collating all connected anomalies and alerts into incidents
- Improve alert fidelity and reduce noise by recognizing and auto-resolving genuine access incidents through identity verification
- Enforce consistent risk-based policies to enable Zero Trust architecture with zero friction actions include block, allow, audit and step up using multifactor authentication (MFA)
- Save log storage costs by storing only relevant authentication logs
- Increase ROI from your MFA investment by extending it to legacy applications and tools

Automate

Enable real-time identity threat detection and protection without time-consuming log processing. Eliminate risky guesswork and prioritize authentication tasks based on over 100 behavior analytics and risk factors for every account.

Hybrid identity store protection: Continuously assess the directory configuration, like Group Policy Objects (GPO), LDAP configurations and risky implementation of protocols like RDP to DC and SMB to DC. Analyze every account from on-premises to hybrid identity stores. Inspect live authentication traffic, including encrypted protocols (e.g., LDAP/S).

Real-time threat detection: Continuously assess identity events and automatically associate them with threats and malicious intent, in real time, without ingesting logs with Falcon Identity Threat Protection's out-of-the-box machine-learning-powered detection rules. With advanced analytics and patented machine learning, uncover reconnaissance (e.g., LDAP, BloodHound, SharpHound, credential compromise attacks), lateral movement (e.g., RDP, pass-the-hash (PtH), Mimikatz tool, unusual endpoint usage, unusual service logins, etc.), and persistence (e.g., Golden Ticket attack, privilege escalation, etc.).

Intuitive threat hunting: Investigate faster with unified domain access into detailed activities of every account across hybrid identity stores without the need for complex, string-based queries. Choose from a list of predefined search criteria, including authentication events, use of unencrypted protocols, user roles, IP reputation, risk scores and many more. Safely lure adversaries with honeytoken accounts and get dedicated insights into their attack paths. If required, create and save your own search criteria to proactively sift through raw events and email them as periodic reports.

Comprehensive API coverage: Extend the Falcon platform's risk score and high-fidelity information to other apps (e.g., AD FS, SSO, IT systems and over 50 integrations) with minimal effort using API-based connectors.

Verify

Secure employee or contractor access to applications, tools and resources with a zero-friction user experience. Ensure consistent login experience for genuine users, but automatically step up authentication when risk scores increase.

Zero-friction identity verification with flexible policies: Define and enforce access policies with simple rules with Falcon Identity Threat Protection adaptive analysis, eliminating the need to write complex static conditions for every user. The policies are based on authentication patterns, behavior baselines, individual user risk score and device risk score (via API integration) to verify identities using MFA. This robust methodology secures access to identity stores and applications, with improved user experience — e.g., identity verification is triggered only when the risk increases or if there's a deviation from normal behavior.

Improved security posture with extended MFA: Extend identity verification/MFA to any resource or application, including legacy/proprietary systems and tools that traditionally could not be integrated with MFA — for example, desktops that are not covered by cloud-based MFA solutions, and tools like PowerShell and protocols like RDP over NTLM — to reduce the attack surface.

Auto-resolve security incidents: With the platform's customizable enforcement policies, resolve standard incidents that the user approves using identity verification methods (2FA/MFA), so that your security analysts can focus on critical security incidents. Additionally, resolve these incidents with effortless API integrations into SOAR, SIEM and ticketing platforms.

Frictionless AD security

- **Multi-directory identity layer support:** Falcon Identity Threat Protection supports Microsoft AD and Entra ID, protects the weakest link in your identity defenses and delivers strong identity with SSO and federation solutions like Okta, AD FS and Ping Identity.
- **Broad MFA support:** Falcon Identity Threat Protection supports multiple MFA solutions, including Okta, Entra ID, Duo, RSA, PAM, Push and more.
- **Extended protocol coverage:** Falcon Identity Threat Protection provides granular visibility and control over encrypted protocols like NTLM and LDAPS, which are difficult to detect with traditional tools like SIEM and UEBA.
- **Extensive API coverage:** Falcon Identity Threat Protection enables over 50 integrations with API-based connectors, providing easy integration with identity as a service (IDaaS)/SSO, SIEM, SOAR, ticketing and asset management solutions.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

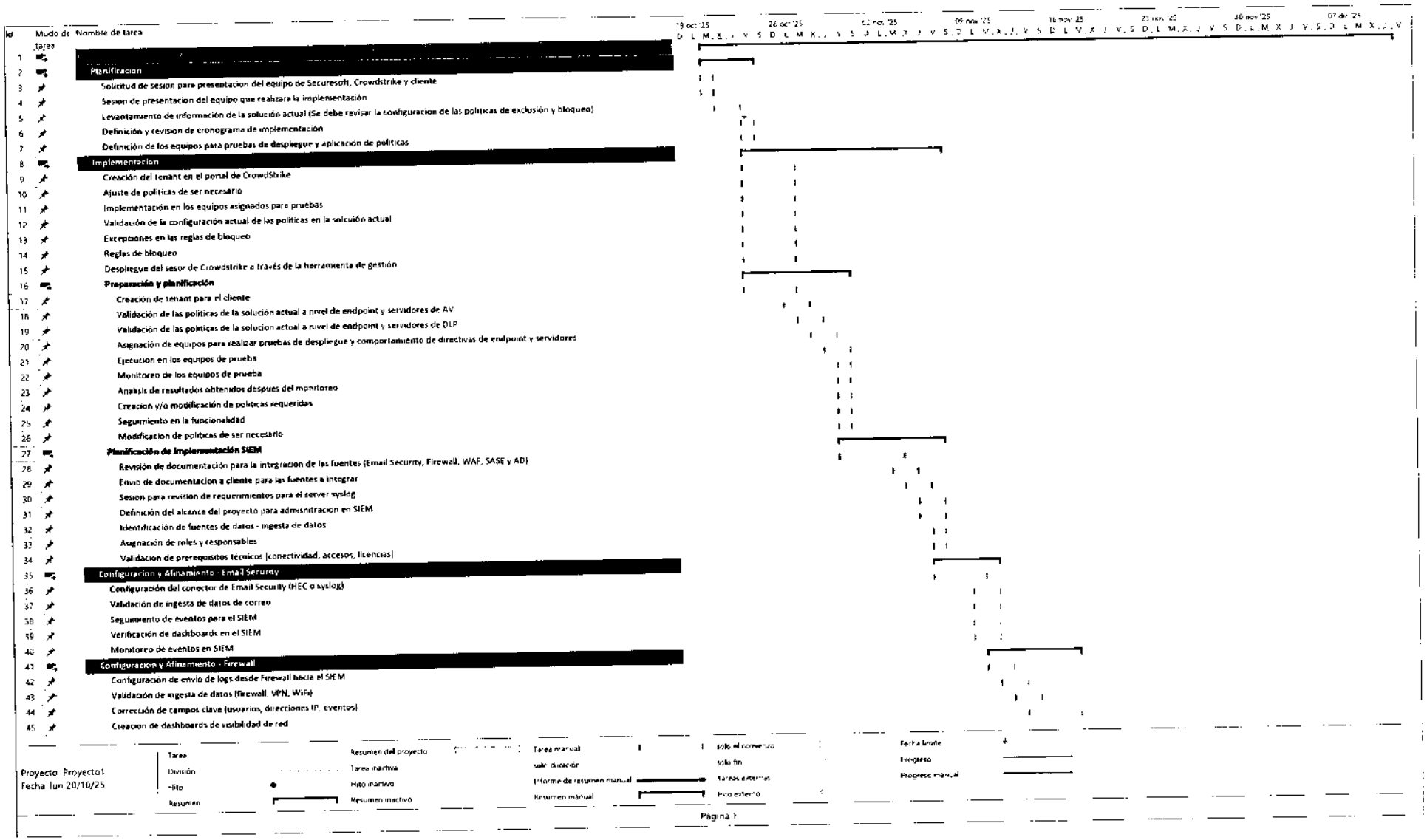
Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

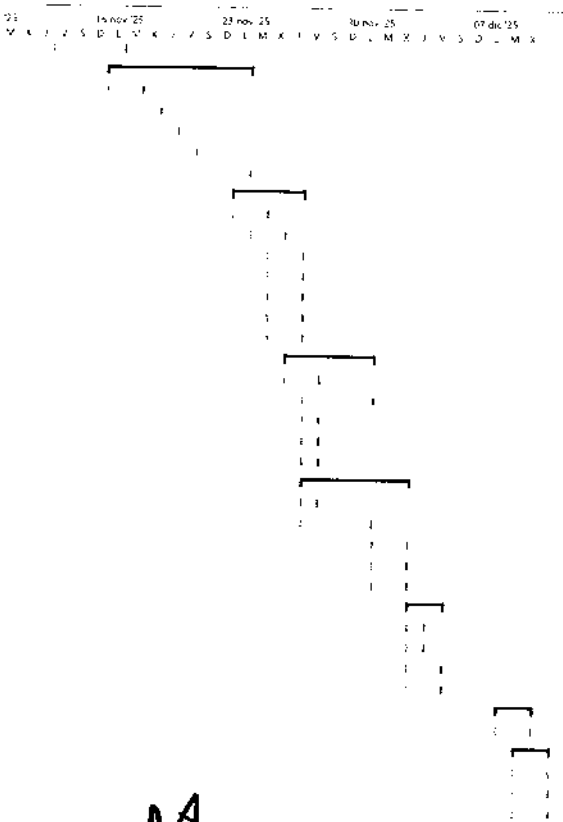
CrowdStrike: We stop breaches.

Start a Free Trial →

© 2024 CrowdStrike, Inc.


Id
Modo de tarea
Nombre de tarea
19 oct '25
26 oct '25
02 nov '25
09 nov '25
16 nov '25
23 nov '25
30 nov '25
07 dic '25
1 Planificacion
2 Planificacion
3 Solicitud de sesion para presentacion del equipo de Securesoft, Crowdstrike y cliente
4 Sesion de presentacion del equipo que realizara la implementación
5 Levantamiento de información de la solución actual (Se debe revisar la configuracion de las politicas de exclusión y bloqueo)
6 Definición y revison de cronograma de implementación
7 Definición de los equipos para pruebas de despliegue y aplicación de politicas
8 Implementacion
9 Creación del tenant en el portal de CrowdStrike
10 Ajuste de politicas de ser necesario
11 Implementación en los equipos asignados para pruebas
12 Validación de la configuración actual de las politicas en la solución actual
13 Excepciones en las reglas de bloqueo
14 Reglas de bloqueo
15 Despliegue del sesor de Crowdstrike a través de la herramienta de gestión
16 Preparación y planificación
17 Creación de tenant para el cliente
18 Validación de las políticas de la solución actual a nivel de endpoint y servidores de AV
19 Validación de las políticas de la solucion actual a nivel de endpoint y servidores de DLP
20 Asignación de equipos para realizar pruebas de despliegue y comportamiento de directivas de endpoint y servidores
21 Ejecucion en los equipos de prueba
22 Monitoreo de los equipos de prueba
23 Analsis de resultados obtenidos despues del monitoreo
24 Creacion y/o modificación de politicas requeridas
25 Seguimiento en la funcionalidad
26 Modificacion de politicas de ser necesario
27 Planificación de implementación SIEM
28 Revisión de documentación para la integracion de las fuentes (Email Security, Firewall, WAF, SASE y AD)
29 Envio de documentacion a cliente para las fuentes a integrar
30 Sesion para revision de requerimientos para el server syslog
31 Definición del alcance del proyecto para administracion en SIEM
32 Identificación de fuentes de datos - ingesta de datos
33 Asignación de roles y responsables
34 Validacion de prerequisitos técnicos (conectividad, accesos, licencias)
35 Configuracion y Afinamiento - Email Security
36 Configuración del conector de Email Security (HEC o syslog)
37 Validación de ingesta de datos de correo
38 Seguimiento de eventos para el SIEM
39 Verificación de dashboards en el SIEM
40 Monitoreo de eventos en SIEM
41 Configuracion y Afinamiento - Firewall
42 Configuración de envio de logs desde Firewall hacia el SIEM
43 Validación de ingesta de datos (firewall, VPN, WiFi)
44 Corrección de campos clave (usuarios, direcciones IP, eventos)
45 Creacion de dashboards de visibilidad de red
Proyecto: Proyecto1
Fecha: lun 20/10/25
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
Solo duración
Informe de resumen manual
Resumen manual
Solo el comienzo
Solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 1

Id	Modo de tarea	Nombre de tarea
46		Monitoreo de eventos en SIEM
47		**Configuracion y Afinamiento - WAF**
48		Configuración del conector WAF
49		Validación de ingesta de datos
50		Seguimiento de eventos para el SIEM
51		Verificacion de dashboards en el SIEM
52		Monitoreo de eventos en SIEM
53		**Configuracion y Afinamiento - SASE**
54		Configuración de conector SASE
55		Validación de logs de navegación
56		Ajuste de parsing y categorización en SIEM
57		Creación de alertas para tráfico sospechoso
58		Seguimiento de eventos para el SIEM
59		Verificación de dashboards en el SIEM
60		Monitoreo de eventos en SIEM
61		**Configuracion y Afinamiento - AD**
62		Configuración del conector AD
63		Validacion de ingesta de datos
64		Seguimiento de eventos para el SIEM
65		Verificación de dashboards en el SIEM
66		Monitoreo de eventos en SIEM
67		**Pruebas y Validacion**
68		Simulación de incidentes de seguridad (correo, navegación, red)
69		Validacion de correlación entre las fuentes
70		Ajuste de alertas para reducir falsos positivos
71		Validacion con SOC y proceso de alestamiento
72		Documentación de resultados de las pruebas
73		**Dashboards iniciales y alertas**
74		Creación de dashboards para informes y analistas
75		Configuración de alertas en tiempo real
76		Validación de reportes automaticos para cliente
77		Desarrollo casos de uso
78		**Capacitacion**
79		Capacitación del equipo
80		**Cierre**
81		Elaboración de documentación de implementación
82		Entrega de documentacion de cierre de implementacion del proyecto
83		Reunión de cierre de implementacion del proyecto



JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

JOSE FRANCISCO LOMBANA CARDONA
C. C.14.395.966
Supervisor Contrato No. 259/2025

Proyecto: Proyecto1
Fecha: lun 20/10/25

Tarea | División | Hito | Resumen | Resumen del proyecto | Tarea externa | Hito inactivo | Resumen inactivo | Tarea manual | Solo duración | Informe de resumen manual | Resumen manual | Solo el comienzo | Solo fin | Tareas externas | Hito externo | Fecha límite | Progreso | Progreso manual

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: COMPROMISO DE EJECUCIÓN A TODO COSTO Y ALCANCE DEL SERVICIO

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del **CONTRATO No. 259COGFM DIADF 2025, la UT 273COGFM H&Y 2025**, en calidad de Contratista, manifiesta formalmente que la ejecución del contrato se realizará **a todo costo**, entendiendo por ello que serán de su exclusiva responsabilidad todos los gastos, recursos, actividades, personal, herramientas, licencias, materiales y demás elementos necesarios para la correcta prestación del servicio.
El Contratista se compromete a:

1. **Prestar el servicio objeto del contrato** incluyendo, de manera integral, las actividades de **instalación, configuración, implementación y puesta en marcha** de la solución contratada.
2. **Realizar las pruebas de funcionalidad necesarias** para verificar el correcto desempeño de la solución, dejando evidencia de las **pruebas exitosas de funcionalidad** y asegurando que el servicio quede plenamente operativo conforme a las especificaciones técnicas y a los requerimientos del supervisor del contrato.
3. Asumir todos los costos y recursos requeridos para atender las obligaciones aquí descritas, sin que ello genere costos adicionales para la Entidad Contratante, salvo los expresamente pactados en el contrato principal.

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

COMPROMISO CONFIDENCIALIDAD

SERA DILIGENCIADO AL MOMENTO DE SUSCRIPCIÓN DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mi propio nombre y de los funcionarios o asesores que se vinculen a la misma para efectos de ejecución del presente contrato, asume el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que el **MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA** adelantó el proceso de selección del Contrato de No. 259 , cuyo objeto es PRESENTE CONTRATO, EL CUAL SE REGIRÁ POR LAS SIGUIENTES: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA SE OBLIGA PARA CON EL MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES-DIRECCIÓN ADMINISTRATIVA Y FINANCIERA A PRESTAR EL SERVICIO DE MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM PARA EL LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS Y LOTE 5: SUSCRIPCIÓN WAF, DE CONFORMIDAD CON LAS ESPECIFICACIONES TÉCNICAS, ASPECTOS TÉCNICOS PONDERABLES, PERSONAL PARA LA EJECUCIÓN DEL CONTRATO Y CUADRO DE PRECIOS DESCRITOS EN EL ANEXO ÚNICO.

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares del Ministerio a los cuales tenga acceso.

CUARTA: Que acepto y permito al Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, utilizar de manera responsable y de acuerdo con la política de protección de datos personales, la información que he proporcionado, para lo cual garantizó que son exactos, por lo que, en caso de ser modificados, comunicaré al Ministerio, para que sean rectificados y/o cancelados según proceda.

QUINTA: Que, por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:

CLÁUSULA PRIMERA. COMPROMISO ASUMIDO POR EL CONTRATISTA: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

EL CONTRATISTA se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.

b) No permitir que terceros obtengan información relacionada con el literal anterior.

c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

e) No dar, ofrecer dadivas, regalos, beneficios, comisiones, promesa remuneratoria, directa o indirectamente; tanto en el ministerio o fuera de él, a cambio de obtener beneficios ilegales en la ejecución de sus obligaciones contractuales.

f) Fomentar el reporte de conductos, hechos que puedan llegar a configurasen en prácticas de soborno, corrupción, con fundamento en la buena fe o en una sospecha razonable.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: EL CONTRATISTA asume a través de la suscripción del presente compromiso, las consecuencias que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente EL CONTRATISTA que toda la información que se produzca en la ejecución del contrato será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá, D.C. a los (09) días del mes de julio del dos mil veinticuatro (2025).

EL CONTRATISTA

Nombre: JESÚS ALBERTO FRANCO ACOSTA
C.E. No. 582410

Este anexo hará parte integral del contrato respectivo.

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: Entrega de Ponderables – Contrato No. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del Contrato No. 259COGFM DIADF 2025, la Unión Temporal UT273COGFM H&Y 2025, en calidad de Contratista, manifiesta formalmente su compromiso de garantizar la correcta prestación del Servicio de Suscripción Plataforma Protección de Datos – Lote No. 3.

En atención al requerimiento de entrega de los ponderables correspondientes, se informa que se ha realizado la entrega efectiva de los compromisos establecidos, conforme se detalla a continuación:

1	**El contratista ofrece sin costo adicional:** Transferencia de conocimiento de la solución de protección de datos ofertada con certificación de Voucher para cuatro (4) funcionarios del Comando General de las Fuerzas Militares – CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM	1	$20,749,691.32	20,749,691.32

De esta manera, la Unión Temporal UT273COGFM H&Y 2025 ratifica el cumplimiento de los compromisos adquiridos y reitera su disposición para atender cualquier requerimiento adicional que contribuya al correcto desarrollo del contrato

Yeapdata®

Heimcore

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410

Carlos Giovani Diaz Rueda

De: Alejandro Gonzalez <alejandro.gonzalez@crowdstrike.com>
Enviado el: miércoles, 10 de diciembre de 2025 09:42 a. m.
Para: Carlos Giovani Diaz Rueda
CC: Andres Rodrigo Rodriguez Castañeda
Asunto: Re: [External] Transferencia de conocimiento - Voucher para cuatro (04) funcionarios - Crowdstrike

Hola

La información completa

Thanks for reaching out.

Please find your account's exam voucher codes below. Additionally, please ensure they are used to both schedule and attend exams occurring prior to the expiration date listed.

Voucher Code	Voucher Expiration Date	Voucher Status
CSPU382B5D0A	10/30/2026	Available
CSPU39223D4E	10/30/2026	Available
CSPU39293A1D	10/30/2026	Available
CSPU39989D93	10/30/2026	Available

Please follow these steps when you're ready to take your CrowdStrike Certification Exam:

1. Sign in to CrowdStrike University
    - If this is your first time taking a CrowdStrike certification exam, find your CrowdStrike University ID on your profile page and make note of it – you will need to input this when you create your exam taker account with Pearson VUE
2. Select Prepare and Get Certified from the CrowdStrike University homepage
3. Select Schedule your certification exam, which will redirect you to the Pearson VUE/CrowdStrike website where you can create your exam taker account and register for your exam
    - If you encounter any scheduling issues online, you may call Pearson VUE at 866-980-0413 to schedule your exam
4. When creating your exam taker account profile, be sure to add your CrowdStrike University ID

Yeapdata®

Heimcore

Bogotá, 04 de diciembre de 2025

Señores
Comando General de las Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá

Asunto: Entrega de Ponderables – Contrato No. 259COGFM DIADF 2025

Respetados señores:

En cumplimiento de las obligaciones contractuales derivadas del Contrato No. 259COGFM DIADF 2025, la Unión Temporal UT273COGFM H&Y 2025, en calidad de Contratista, manifiesta formalmente su compromiso de garantizar la correcta prestación del Servicio de Suscripción WAF – Lote No. 5.

En atención al requerimiento de entrega de los ponderables correspondientes, se informa que se ha realizado la entrega efectiva de los compromisos establecidos, conforme se detalla a continuación:

1	**El contratista ofrece sin costo adicional:** Terminal para administración y gestión de la solución de seguridad que debe incluir como mínimo Intel® Core™ Ultra 7 265KF, Windows 11 Pro, NVIDIA® GeForce RTX™ 5080, 32 GB DDR5, SSD de 2 TB, con periféricos incluidos y 02 dispositivos de visualización de 25" que permitan visualización y monitoreo de datos críticos, sin que este ofrecimiento genere costo adicional para la entidad.	1	$ 21,441,865.52	$ 21,441,865.52

De esta manera, la Unión Temporal UT273COGFM H&Y 2025 ratifica el cumplimiento de los compromisos adquiridos y reitera su disposición para atender cualquier requerimiento adicional que contribuya al correcto desarrollo del contrato

Sin otro particular, agradecemos su atención y quedamos atentos a cualquier inquietud adicional.

Atentamente,

JESUS ALBERTO FRANCO ACOSTA
REPRESENTANTE LEGAL UT273COGFM H&Y 2025
C.E. 582410