FECHA: 6 de marzo de 2024

PARA: **JOHANNA PIMIENTO QUINTERO**
Directora Unidad de Transformación Digital e Informática

DE: **FRANCISCO JAVIER GONZÁLEZ MÉNDEZ**

Asunto: Informe de entrega de supervisión de contrato 227 servicios ECMR de 2024.

En atención al desarrollo de la ejecución del contrato 227 de 2024 de servicios ECMR, me permito anexar al presente un informe de ejecución de este, con el propósito de cumplir el requisito para la entrega de supervisión del contrato a la Directora de la Unidad de Transformación Digital, Ingeniera Johanna Pimiento Quintero.

Lo anterior en razón que desde el pasado 3 de marzo de 2025 renuncié al cargo que desempeñaba como Director Administrativo de la División de Seguridad de Información y Protección de Datos.

Cordialmente,

FRANCISCO JAVIER GONZÁLEZ MÉNDEZ

Elaboró: Francisco Javier González Méndez

ANEXO

DIRECCION EJECUTIVA DE ADMINISTRACION JUDICIAL INFORME ENTREGA SUPERVISION TECNICA
DATOS DEL INFORME

Fecha Informe: 06/03/2025 **Periodo Informe:** 01/01/2025 - 03/03/2025 **Nombre del Contratista:** Ernst & Young SAS

CONTRATO: 227 de 2024 – Otro

OBJETO:
Adquirir la suscripción de los servicios especializados de un Equipo Central de Monitoreo y Reacción (ECMR), con el fin de supervisar activos tecnológicos, gestionar vulnerabilidades, analizar amenazas y responder en tiempo real a incidentes

Rubro	**Vigencia**	**CDP N°**	**Fecha CDP**	**Valor Total**
27-01-02-032 recursos BID	2024	57124 y 12324	2024-12-05 2024-12-05	$1.946.511.982 $635.000.000
			TOTAL	**$2.581.511.982**

Pagos realizados: ninguno

EJECUCIÓN DE ACTIVIDADES

Obligaciones Contractuales

1. Prestar los servicios 7x24x365 durante la suscripción del servicio.
2. El proveedor debe contar con procesos de contingencia y continuidad para la prestación del servicio requerido.
3. Presentar el plan de trabajo a la supervisión del contrato.
4. Supervisar todos los sistemas de la Rama Judicial para detectar o identificar violaciones de seguridad.
5. Realizar el manejo de incidentes realizando el triage de los incidentes de seguridad, correlación de eventos, respuesta ante incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la organización mediante medición de ANS.
6. Realizar la identificación, análisis, escalamiento, reporte de los casos, acciones de tratamiento e indicadores de compromiso y seguimiento de las alarmas, eventos e incidentes de seguridad de la información detectados.
7. Debe mantenerse actualizado de manera continua sobre las nuevas vulnerabilidades y las estrategias de ataque empleadas por los atacantes, con el fin de estar al tanto de las últimas modalidades de ciberataques que podrían afectar a la entidad y, en consecuencia, reportarlas de forma oportuna.
8. Investigar nuevos parches de software.
9. Documentar, catalogar, investigar y hacer seguimiento a los incidentes y/o incidentes de seguridad.
10. Generar y socializar la evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos de la Rama Judicial, esto debe implementar actividades de Ethical Hacking y presentar los resultados al Grupo de proyectos Especiales de Tecnología y a la Unidad Informática.
11. Analizar, establecer, generar y supervisar las posibles amenazas, riesgos, exposiciones y pérdidas que puedan resultar del acceso no autorizado datos, programas, terminales, periféricos y demás activos de información de la Rama Judicial para determinar

Actividades Realizadas

Desde el 31 de diciembre del 2024 hasta el 28 de febrero el Ernst & Young SAS ha realizado las actividades de monitoreo de la infraestructura tecnológica de la Rama Judicial de acuerdo con lo establecido en el contrato.

En las actividades realizadas en los dos primeros meses del año 2025 el contratista EY SAS entregó los servicios de acuerdo con las obligaciones del sistema con informe mensual del mes de enero entregado al supervisor del contrato.

Estado de las obligaciones contractuales:

De la obligación 1: los servicios se han venido prestando dese enero 1 de 2025 hasta la fecha y en modalidad 7x24x365 sin ninguna novedad para la ejecución.

De la obligación 2: el proveedor cuenta con procesos de contingencia y continuidad para la prestación del servicio requerido.

De la obligación 3: el proveedor presentó un plan de trabajo para el periodo de ejecución del contrato. Este documento se encuentra en el repositorio sharepoint de la División de Seguridad.

De la obligación 4: actualmente el servicio realiza la supervisión de todos los sistemas de la Rama Judicial con el fin de detectar o identificar violaciones de seguridad; esto se puede evidenciar en los informes mensuales de gestión entregados por el contratista y que se encuentran en el repositorio sharepoint de la División de Seguridad.
.
De la obligación 5: para los 2 meses de ejecución del contrato (enero y febrero de 2025) se presentaron dos incidentes de seguridad atendidos y resueltos; se cuenta y se aplica el procedimiento de gestión de incidentes. De igual forma el contratista a través del ECMR ha venido realizando la correlación de eventos, que se producen desde las distintas fuentes de información que se integran al

SC5780-4 CO-SA-CER551308

medidas preventivas y correctivas.
12. Generar, socializar e implementar la Gestión de Riesgos de la Seguridad Informática y de la Información.
13. Analizar los riesgos de seguridad de la información, así como definir los tratamientos establecidos para los riesgos analizados y evaluados.
14. Analizar y monitorear los registros de eventos con la relación a las operaciones de los usuarios sobre los sistemas y aplicaciones de la Rama Judicial, para identificar comportamientos anómalos y tomar acciones de mitigación de forma oportuna.
15. Debe estar integrado con diferentes organismos de respuesta a incidentes de seguridad y fuentes de inteligencia (policía, ejercito, entidades especializadas en ciberseguridad) y servir como punto central de comunicación, tanto para recibir informes de incidentes de seguridad como para difundir información crucial a las entidades apropiadas sobre el incidente.
16. Clasificar y priorizar las alarmas, eventos e incidentes detectados y analizarlos con el fin de poder determinar sus causas, origen e impacto en coordinación con los grupos internos.
17. El servicio de gestión de alertas, eventos e incidentes de seguridad deberá contemplar el escalamiento y seguimiento de los casos detectados de acuerdo con el protocolo que se establezca para tal fin y debe estar alineados con los grupos internos de la Rama Judicial.
18. Deberá realizar el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente, esta debe estar incluidas en una plataforma donde se pueda realizar el seguimiento, actividades realizadas hasta el cierre de las mismas, donde la Rama Judicial tenga acceso, para el seguimiento de los mismo a través de Dashboards e informes mensuales.
19. El servicio deberá estar en la capacidad de definir y configurar tipos de alertas y alertas de acuerdo con el nivel de criticidad de los eventos e incidentes de seguridad de la información y ciberseguridad.
20. Cumplir con estándares de seguridad de la información.
21. Monitorear los componentes de la infraestructura tecnológica implementada para la prestación de los servicios de forma proactiva mediante herramientas de gestión y deberán incluir las actividades del ECMR y el monitoreo de eventos de seguridad y de disponibilidad que afecten a la entidad.
22. Realizar los mantenimientos preventivos y correctivos adecuados para asegurar la continua disponibilidad e integridad de la infraestructura de los servicios en coordinación con los grupos internos.
23. Emplear múltiples metodologías de detección para descubrir actividad maliciosa:
a. Análisis de comportamiento del usuario (UEBA): Este crea una línea de base de la
actividad normal del usuario dentro de su entorno y genera pistas de investigación
cuando hay una desviación.
b. Analítica de comportamiento de Atacantes (ABA): Aplica análisis de
comportamiento para generar investigaciones, construidas a partir de la
experiencia y comprensión de las herramientas, tácticas y metodologías de los

correlacionador de eventos de la herramienta de ciberseguridad Rapid 7.

De la obligación 6: para los 2 meses de ejecución del contrato (enero y febrero de 2025) el ECMR ha venido realizando la identificación, análisis, escalamiento, reporte de los casos, acciones de tratamiento e indicadores de compromiso y seguimiento de las alarmas, eventos detectados a través de la herramienta de ciberseguridad Rapid 7. Es de anotar que no se han presentado incidentes de seguridad de la información.

De la obligación 7: se han realizado mantenimientos de manera continua sobre las nuevas vulnerabilidades.

De la obligación 8: se han realizado las investigaciones nuevos parches de software.

De la obligación 9: se ha realizado la documentación, se catalogaron, investigar y hacer seguimiento a los incidentes y/o incidentes de seguridad.

De la obligación 10: Durante los meses de enero y febrero de 2025 se generaron evaluaciones de vulnerabilidades en los servicios tecnológicos / sistemas de información localizados en las nubes públicas de AWS y Azure. Como resultado de estas evaluaciones se produjeron informes de vulnerabilidades que fueron enviados y socializados a los lideres técnicos responsables de los servicios tecnológicos/sistemas de información para su remediación.

De la obligación 11: El proveedor ha estado realizando análisis de posibles amenazas, riesgos, exposiciones y pérdidas que puedan resultar del acceso no autorizado datos, programas, terminales, periféricos y demás activos de información de la Rama Judicial y a enviado medidas preventivas y correctivas para mitigar lo identificado.

De la obligación 12: El proveedor ha estado generado, socializado e implementado la Gestión de Riesgos de la Seguridad Informática y de la Información que atañen al servicio del ECMR.

De la obligación 13: Los riesgos identificados de seguridad de la información están siendo tratados.

De la obligación 14: El proveedor realiza análisis y monitoreo de los registros de eventos con la relación a las operaciones de los usuarios sobre los sistemas y aplicaciones de la Rama Judicial, ha identificado comportamientos anómalos e indicado acciones para mitigar lo identificado.

De la obligación 15: El servicio prestado por el proveedor está integrado con diferentes organismos de respuesta a incidentes de seguridad y fuentes de inteligencia (policía, ejercito, entidades especializadas en ciberseguridad).

De la obligación 16: El proveedor clasifica y prioriza las alarmas, eventos e incidentes detectados y los analiza con el fin de poder determinar sus causas, origen e impacto en coordinación con los grupos internos.

De la obligación 17: El servicio de gestión de alertas que realiza el proveedor contempla el escalamiento y seguimiento de los casos detectados de acuerdo con el

atacantes.
c. Detección basada en inteligencia de amenazas: Aprovecha la inteligencia de amenazas derivada de investigaciones, investigaciones previas, hallazgos de monitoreo y fuentes de terceros.
d. Validación humana: los analistas tienen que validar todos los eventos antes de informar incidentes para eliminar alertas benignas, innecesarias o redundantes.
24. El Equipo Central de Monitoreo y Reacción deberá poseer capacidades de búsqueda iterativa y proactiva para la detección y aislamiento de amenazas de ciberseguridad que hayan evadido los controles aplicados en la infraestructura. Las capacidades de CYBER THREAT HUNTING deben utilizar el modelo de ataque MITRE 's ATT&CK lifecycle el cual constituye una base de datos de las técnicas y tácticas de los ciber atacantes.
25. El servicio debe contar con capacidades de CYBER THREAT INTELLIGENCE para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques, amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad.
26. El proveedor deberá establecer un procedimiento apoyado con buenas prácticas, CSIRT gubernamental para la detección, alertamiento, notificación y seguimiento de eventos o incidentes de seguridad; también para informar puntos débiles de seguridad; definir responsabilidades que se deberían asignar para la gestión de incidentes y proponer mejoras de seguridad de la información.
27. El proveedor del Equipo Central de Monitoreo y Reacción tiene que contar con un equipo de Inteligencia de amenazas que utiliza una combinación de hallazgos internos y fuentes de amenazas de terceros para la inteligencia. La información de las fuentes de información externa que alimenta la analítica y los datos adicionales de productos y servicios debe permitir que el equipo sea proactivo en relación con las amenazas y los datos de amenazas. El equipo de Inteligencia de amenazas del proveedor del ECMR debe escribir un informe acorde al SGSI de amenazas para compartir tendencias sobre las mismas.
28. Deberá emplear, como mínimo, las siguientes metodologías para llevar a cabo actividades de cacería de amenazas (threat hunting).
29. El contratista se puede apoyar en las herramientas ya instaladas en la Rama Judicial y se requiere que el contratista instale todos los componentes que sean requeridos para cumplir con el presente anexo técnico y los servicios requeridos por la entidad de manera autónoma sin generar dependencia de los servicios y herramientas actuales que se encuentran instaladas.
a. Análisis de comportamiento del usuario (UBA): el motor UBA atribuye la actividad a los usuarios finales, creando una línea base de actividad regular para todos y cada uno de los usuarios en la red. Las alertas UBA identifican el uso anómalo, sospechoso y malicioso de las credenciales de usuario y los derechos de administrador, incluyendo ingreso sospechoso a la red, intentos de fuerza bruta, movimiento lateral, escalada de privilegios y acceso a segmentos, servidores y archivos críticos de la red.
b. Detección y respuesta de punto final: El Agente captura eventos de actividad de proceso en tiempo protocolo establecido para tal fin y esta alineado con los grupos internos de la Rama Judicial.

De la obligación 18: El proveedor ha realizado seguimiento a los eventos hasta que estos se han cerrados adecuada y oportunamente, así mismo se hace seguimiento de estos a través de Dashboards e informes mensuales

De la obligación 19: El proveedor ha definido y configurado diferentes tipos de alertas de acuerdo con el nivel de criticidad de los eventos e incidentes de seguridad de la información y ciberseguridad.

De la obligación 20: El proveedor cumple con estándares de seguridad de la información como ISO27001 y NIST.

De la obligación 21: El proveedor monitorea los componentes de la infraestructura tecnológica implementada para la prestación de los servicios de forma proactiva mediante herramientas de gestión.

De la obligación 22: se realizan constante revisión y monitoreo de la infraestructura de ciberseguridad que se tiene instalada actualmente en nube pública de AWS, lo cual permite el seguimiento al adecuado funcionamiento de los servicios de ciberseguridad.

De la obligación 23: el ECMR aplica constantemente UEBA para el análisis del comportamiento de usuarios y entidades, utilizando el aprendizaje automático (ML), el aprendizaje profundo y el análisis estadístico para identificar los patrones de comportamiento normales de usuarios y entidades (por ejemplo, hosts, aplicaciones, tráfico).

De la obligación 24: El ECMR utiliza las capacidades de búsqueda iterativa y proactiva para la detección y aislamiento de amenazas de ciberseguridad que hayan evadido los controles de Firewall aplicados en la infraestructura. También se utiliza el modelo de ataque MITRE 's ATT&CK para el modelado de amenazas y la defensa de la seguridad con el fin de comprender mejor los riesgos de seguridad asociados con amenazas específicas y mejorar las estrategias de detección y prevención.

De la obligación 25: el ECMR realiza actividades de cyber threat intelligence para el monitoreo y alertamiento temprano de nuevas vulnerabilidades, ataques, amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la rama judicial.

De la obligación 26: El proveedor cuenta con un procedimiento con buenas prácticas, apoyándose con el CSIRT gubernamental para la detección, alertamiento, notificación y seguimiento de eventos o incidentes de seguridad; también para informar puntos débiles de seguridad; se cuenta con responsabilidades asignadas para la gestión de incidentes y proponer mejoras de seguridad de la información.

De la obligación 27: El proveedor cuenta con un equipo de Inteligencia de amenazas que utiliza una combinación de hallazgos internos y fuentes de amenazas de terceros para la inteligencia. El equipo de Inteligencia de amenazas reporta constantemente situaciones identificadas.

icontec ISO 9001 SC5780-4 IQNet icontec ISO 14001 CO-SA-CER551308

real, que son analizados. Estos datos de proceso se usan para alertar sobre hashes de procesos maliciosos conocidos, patrones de ejecución de procesos sospechosos, uso malicioso de herramientas de línea de comandos, evidencia de intentos de persistencia adversos, y más. Esta base de datos de comportamientos de atacante debe ser depurada por el propio equipo de investigación de amenazas y CMR administrado para mantener el ritmo de las tácticas, técnicas y procedimientos modernos de ataque.
c. Tecnología de engaño/Deception: El servicio del Equipo Central de Monitoreo y Reacción tiene que incluir trampas para intrusos diseñadas para capturar la actividad del atacante que rara vez, si alguna vez, aparece en los datos de registro. Estas trampas incluyen honeypots, usuarios señuelo, archivos señuelos y credenciales señuelos.
d. Inteligencia de amenazas: Debe incluir una fuente depurada de inteligencia de amenazas proporcionada por el propio Equipo Central de Monitoreo y Reacción y el grupo de investigación de amenazas junto con la Alianza de amenazas cibernéticas (CTA) o entidades similares. Esta inteligencia de amenazas debe incluye hashes de procesos maliciosos, direcciones IP, dominios y URL. Las alertas se tienen que generar automáticamente si cualquier evento de registro analizado contiene un indicador de compromiso (IOC) rastreado en la inteligencia de amenazas, y la entidad también podrá cargar sus propias fuentes de información de amenazas personalizados para rastrear IOC adicionales. • Alertas personalizadas: además de las alertas nativas descritas anteriormente, se requiere que la entidad pueda usar el motor de búsqueda de registros para crear alertas personalizadas. La configuración de Alertas personalizadas debe permite crear alertas directamente desde la página de búsqueda de registros y admitir dos tipos de alertas personalizadas: Alertas de detección de inactividad y Alertas de detección de cambios. También debe tener métodos de notificación, que incluyan notificaciones por correo electrónico y Microsoft Teams, o el canal que provea el contratista.
30. Dentro del servicio del Equipo Central de Monitoreo y Reacción, se requiere contar con la posibilidad de crear reglas personalizadas que cumplan con:
a. Alertas de detección de inactividad: también conocidas como " Monitoreo hacia arriba y hacia abajo ", deben usarse para notificar cuando un registro completo, un grupo de registros o un patrón particular se vuelve inactivo durante un periodo de tiempo determinado. La alerta de inactividad es útil para los activos del sistema que deben ejecutarse constantemente (como un servidor crítico). La capacidad de establecer la ventana de tiempo de inactividad da control sobre los datos, el entorno y los activos, permite el control de danos y la prevención de la pérdida de datos.
b. Alertas de detección de patrones: Para que se active una alerta, un registro debe coincidir con el patrón exacto que ingresó como término de búsqueda. Alertar sobre patrones puede ser útil en situaciones como la supervisión de errores en servidores, excepciones críticas y rendimiento general, y permite

De la obligación 28: se realizan actividades de cacería de amenazas (threat hunting), a través de la herramienta Rapid

De la obligación 29: El proveedor se utiliza las herramientas ya instaladas en la Rama Judicial (Rapid 7), así mismo esta utilizando la herramientas de:
a. Análisis de comportamiento del usuario (UBA).
b. Detección y respuesta de punto final.
c. Tecnología de engaño/Deception.
d. Inteligencia de amenazas

De la obligación 30: Dentro del servicio del Equipo Central de Monitoreo y Reacción, se cuenta con reglas personalizadas:
a. Alertas de detección de inactividad.
b. Alertas de detección de patrones.
c. Alertas de detección de cambios.

De la obligación 31: el Equipo Central de Monitoreo y Reacción, cuenta con las siguientes protecciones:
a. Para los datos en reposo.
b. Datos en tránsito.
c. Sin embargo, la Rama no cuenta con una herramienta de DLP que el ECMR pueda monitorear.

De la obligación 32: el servicio del Equipo Central de Monitoreo y Reacción cuenta con capacidad de respuesta con las siguientes características:
a. Acciones de respuesta en nombre de la entidad.
b. Respuesta de usuarios o credenciales.
c. El tiempo para proponer la acción es inmediatamente.
d. El proveedor utiliza la herramienta de ticket de la entidad
e. El proveedor cuenta con tableros de control en la herramienta R7 y también en tableros desarrollados en Power BI.

Como punto de alerta se pone de presente que la licencia de la herramienta Rapid 7 entregada por la Rama Judicial a Ernst & Young SAS vence al 31 de marzo de 2025 y el no contar on la continuidad de esta herramienta o de otras herramientas de seguridad que la suplan dificultaría el cumplimiento del contrato 227/2024.

monitorear solo eventos que son importantes para la entidad.
c. Alertas de detección de cambios: las alertas de detección de cambios notificaran cuando cambie una condición, como los errores HTTP 500 en registros de acceso web. Se basan en los cálculos que aplica a los registros o conjuntos de registros. Las detecciones de cambios ayudaran a estar al tanto de las condiciones críticas cuando algo se dañe y deba abordarse de inmediato, o si ocurren errores que deben escalarse. Esta alerta minimizará el tiempo para investigar y resolver cualquier error.
31. Con el objetivo de garantizar la protección de los datos recopilados por el Equipo
Central de Monitoreo y Reacción, se requieren las siguientes protecciones:
a. Para los datos en reposo: Todos los datos procesados y almacenados se tienen que cifrar en reposo utilizando diversos mecanismos de cifrado a nivel de archivo o disco. Los datos se cifrarán utilizando el cifrado AES-256 estándar de la industria con claves administradas a través del Servicio de administración de claves (KMS)
b. Datos en tránsito: Datos enviados desde y hacia el Equipo Central de Monitoreo y Reacción, incluidos los datos recopilados por recolectores, agentes y motores; datos ingeridos a través de API y complementos; y la interacción con la interfaz de usuario, deben estar encriptados con TLS (HTTPS). Los recopiladores, agentes, motores y complementos tienen que estar configurados para verificar y requieren un certificado TLS valido emitido por una autoridad de certificación de confianza.
c. Hacer uso de la herramienta que prevenga la fuga de información por medio DLP-Data Loss Prevention, provista por la Rama Judicial.
32. Adicionalmente, el servicio del Equipo Central de Monitoreo y Reacción debe contar con capacidad de respuesta bajo las siguientes definiciones:
a. Las siguientes acciones de respuesta se tomarán en nombre de la entidad de acuerdo con las mejores prácticas del Equipo Central de Monitoreo y Reacción y a discreción del equipo responsable del servicio: Respuesta de punto final para amenazas como malware (indicadores de Ransomware, puertas traseras troyanos, etc.) u otras indicaciones de ataque de un atacante. Presencia (evidencia de webshell, etc.) en puntos finales en el entorno, el servicio pondrá en cuarentena un punto final en nombre de la entidad.
b. Respuesta de usuarios o credenciales para amenazas como la actividad del usuario asociada con actividades potencialmente maliciosas, anómalas o sospechosas asociadas con comportamientos comunes de atacantes que aprovechan las credenciales del usuario, el servicio del Equipo Central de Monitoreo y Reacción pondrá en cuarentena a un usuario en nombre de la entidad.
c. El tiempo para proponer la acción es inmediatamente después de que un analista de amenazas valide manualmente la actividad maliciosa o sospechosa para cualquier alerta crítica, el servicio del Equipo Central de Monitoreo y Reacción enviará una acción de respuesta propuesta al cliente a través del servicio provisto por el contratista. Debido a la naturaleza del impacto en los entornos de producción en vivo, el servicio del Equipo Central de Monitoreo y

SC5780-4 CO-SA-CER551308

Reacción debe validar la amenaza antes de tomar la acción. Una vez que se activa a través del servicio provisto por el proveedor, la propuesta de respuesta se establece en un límite de respuesta de 3 minutos ("período de gracia") antes de que el servicio del Equipo Central de Monitoreo y Reacción inicie la acción. La entidad tiene la opción de acelerar o cancelar esta acción de respuesta a través del servicio provisto por el proveedor. La entidad también tiene la opción durante la incorporación para establecer este "período de gracia" en una duración más larga o corta.
d. El proveedor deberá suministrar una plataforma web online (No Excel), donde se pueda verificar los turnos de los diferentes profesionales y las actividades que ejecuta cada uno de ellos en el monitoreo 7x24x365 y asignar usuarios de consulta determinados por la Supervisión del Contrato.
e. El proveedor deberá suministrar una herramienta web online (No Excel), donde se realice el seguimiento de todos los eventos, incidentes, su trazabilidad, proceso de remediación, hasta su cierre. Esta plataforma debe tener usuarios de consulta determinados por la Supervisión del Contrato. Judicial la integración del Modelo de Seguridad y Privacidad de la Información de la Rama Judicial en el marco de los proyectos tecnológicos y no tecnológicos que involucren datos personales.

OBSERVACIONES Y RECOMENDACIONES

En adelante la persona asignada como Director Administrativo - División de Seguridad de la Información quien realice supervisión del contrato 227 de 2024, servidor que debe recibir la información del contrato y el avance del mismo. Cabe resaltar que a la fecha no se presentan atrasos o incumplimiento de las obligaciones por parte del contratista como de la Entidad.

SUSCRIPCIÓN DEL INFORME

Supervisor saliente **FRANCISCO JAVIER GONZALEZ MENDEZ**

Cargo.:
Firma: