1. OBJETO DEL PROCESO

PRESTAR SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA GESTIÓN DE EVENTOS DE CIBERSEGURIDAD DE LA RED DE DATOS

2. OBJETIVO GENERAL

Las presentes especificaciones técnicas detallan los requerimientos, características y condiciones del servicio. Los requerimientos descritos en este anexo técnico son los mínimos exigidos por la Entidad.

El Contratista seleccionado debe comprometerse a proveer un servicio de alta calidad a través de un SOC por fuera de las instalaciones de la entidad (Centro de Operaciones de Seguridad) de propiedad del contratista y ubicado en territorio nacional, con disponibilidad 7x24x365, para la infraestructura tecnológica on-premise y nube de la Aeronáutica Civil, cuya finalidad será implementar procesos de monitoreo para la detección temprana, mediante alertas, de cualquier actividad sospechosa o incidente de seguridad que pudiera comprometer la información de la entidad y cumplir con respuestas efectivas subsanando estos incidentes cumpliendo con los ANS´s respectivos y alineado con las normas ISO 27001:2013 o superior, NIST SP 800-53 Rev. 5.

El objetivo de contrato es contribuir a mejorar la seguridad tecnológica de la Aeronáutica Civil proporcionando un punto central de monitoreo y gestión de todos los aspectos de la seguridad y operatividad tecnológica de la organización, permitiendo tomar acciones preventivas ante amenazas y acciones correctivas de rápida implementación ante incidentes detectados.

El contratista debe cumplir o superar en su totalidad las condiciones técnicas expresadas en el presente documento de especificaciones técnicas Formato 8.

3. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA (RI)

Para cumplir con el objetivo general propuesto el contratista debe cumplir en varios frentes:

- OBLIGACIONES Y REQUERIMIENTOS QUE EL CONTRATISTA DEBE ASEGURAR DEL SERVICIO CONTRATADO (SOC)
  - Obligaciones directas
  - Obligaciones sobre herramientas
  - Plan de comunicaciones
  - Obligaciones sobre Informes y políticas que el contratista debe cumplir.
  - Obligaciones sobre el equipo de trabajo que el contratista debe proveer.

- DETALLES DEL DESARROLLO DEL CONTRATO
  - Fases del contrato
  - Inicio del contrato
  - Ejecución del contrato y prestación del servicio SOC
  - Cierre del contrato y finalización de la prestación del servicio SOC

3.1 OBLIGACIONES Y REQUERIMIENTOS QUE EL CONTRATISTA DEBE ASEGURAR DEL SERVICIO CONTRATADO (SOC)

3.1.1 Obligaciones directas del servicio del SOC

1. El servicio contratado (SOC) debe administrar, gestionar, operar, explotar las herramientas necesarias para correlacionar eventos en tiempo real y cumplimiento de normatividad.

2. El servicio contratado (SOC) debe contar como mínimo con una plataforma SIEM que tenga la capacidad de integrarse con los sistemas que cuenta la Entidad, donde se recopilen eventos en los dispositivos de red, seguridad perimetral, autenticación (Directorio Activo), bases de datos, servidores, aplicaciones y sitios web de la entidad.

3. El servicio contratado (SOC) debe estar dimensionado según los requerimiento y obligaciones redactadas en el presente documento de especificaciones técnicas Formato 8.

4. El servicio contratado (SOC) debe tener un periodo de vigencia sin exceder el 31 de julio de 2026 en un formato de funcionamiento de 7X24X365.

5. Ampliaciones sobre el periodo de vigencia sólo serán aprobadas por mutuo acuerdo entre las partes.

6. Tomando en cuenta que el SOC es un servicio que debe ser Cloud Saas con integración con los módulos on premise de la entidad. El componente Cloud contratado del servicio SOC se debe prestar desde un datacenter con las siguientes características:

   - El datacenter debe tener una capacidad mínima que asegure la disponibilidad y tiempo de funcionamiento requerido por la entidad. En caso de cumplir con una clasificación TIER (1, 2, 3 o más) , el contratista puede incluir su respectiva certificación de Uptime institute o equivalentes, pero el requerimiento que el datacenter tenga una clasificación TIER completamente opcional y no obligatorio.
   - Debe contar con la infraestructura y normatividad vigente a nivel de seguridad informática cumpliendo con lo establecido en la ISO 27001 (2013 o superior o 2022) y la ISO 27032 en cuanto al manejo de incidentes, bajo los siguientes parámetros:
     - El cumplimiento de la ISO 27001 (2013 o superior o 2022) es obligatorio.
     - El cumplimiento de la ISO 27032 puede ser voluntario.
   - Debe tener un funcionamiento 7X24X365 al igual que el servicio contratado.
   - La ubicación del datacenter debe contar con procedimientos, políticas de seguridad física para oficinas, recintos e instalaciones donde se encuentran los equipos, garantizando el esquema de seguridad sobre todos los componentes que integren la solución del servicio, que asegure que el servicio tenga el soporte y pueda garantizar la disponibilidad del servicio contratado (SOC) en un 99,5%.

7. Los proponentes deben entregar en su oferta el **Formato 12 - *Carta de* certificación SOC propio** y adjunto a este formato debe entregar los siguientes certificados (los cuales deben estar vigentes al momento de la presentación de la oferta):
   - ISO27001(2013 o superiores o 2022): El oferente debe presentar junto con su propuesta el certificado ISO 27001(2013 o superiores o 2022) (SGSI) para su proceso de SOC, vigente a la fecha.

   - FIRST: El oferente debe presentar junto con su propuesta el certificado de membresía de FIRST "Forum of Incident Response and Security Teams" (Foro de Equipos de Respuesta a Incidentes y Seguridad) para su proceso de SOC, vigente a la fecha.

   - Certificado de Fabrica: El oferente deberá presentar junto con su propuesta una certificación del fabricante de la solución SIEM y herramientas de ciberseguridad a utilizar que integrará a las plataformas de la entidad para la prestación de los servicios de SOC, vigente a la fecha.

8. El servicio de SOC debe contar con funcionalidades de análisis de comportamiento, detección temprana y avanzada de amenazas y respuesta inteligente a incidentes en una plataforma, cumpliendo los siguientes requerimientos:

- La solución utilizada por los servicios del SOC debe construir automáticamente una base de comportamiento de los usuarios y entidades en la red; basado en un modelo de inteligencia artificial y fundamentado en aprendizaje automático con modelos preconstruidos como el uso de activos, dispositivos, sesiones VPN, accesos físicos, horarios de actividad, uso de correo; etc. Analizando la actividad en la red, así como las sesiones de usuario.
- La solución utilizada por los servicios del SOC, requiere construir automáticamente líneas de tiempo para eventos normales y anormales relacionados a usuarios y entidades centrales, que agilicen la investigación de incidentes; priorizando el nivel de atención de las alertas de seguridad; logrando detectar usuarios comprometidos presentando una imagen integral de su comportamiento, así como contar con la posibilidad de detectar movimientos laterales automáticamente, intercambio de credenciales, direcciones de IP o de dispositivos.

- La solución utilizada por el SOC debe, de manera indispensable, debe asociar eventos que solo contengan el nombre del host o la dirección IP al usuario de manera automática (IP-Host Mapping). Esto permitirá que en ambientes DHCP, se detecte todo movimiento lateral y escalamiento de funciones.
- La solución utilizada por el SOC debe proporcionar, mediante un enriquecimiento de contexto, información de datos sobre un usuario y el evento para su análisis por parte del investigador. Es indispensable la comparación del comportamiento del usuario con otros miembros de su equipo, pares, roles o áreas similares; bajo el contexto de ciencia de datos, detectando así anomalías desde el inicio del aprendizaje.

9. El servicio de SOC debe incluir las siguientes capacidades, incluidos en su solución:
   - Tomando en cuenta que el SOC es un servicio que debe ser Cloud Saas con integración con los módulos on premise de la entidad. El contratista debe tener un componente de infraestructura física propia externa a las instalaciones de la Aerocivil y localizadas en la ciudad de Bogotá D.C y/o sus alrededores, para proveer o monitorear el servicio, garantizando la continuidad y correcta prestación de los servicios. Así mismo, que, para los eventos, ventanas de servicio y cualquier necesidad que se requiera la participación de manera presencial de cualquiera de los roles que presentan el servicio en la entidad, el contratista debe tomar las medidas necesarias para cumplir con lo requerido.
   - Tomando en cuenta que el SOC es un servicio que debe ser Cloud Saas con integración con los módulos on premise de la entidad, El contratista debe asegurar que el componente Cloud de su solución impida que la información de la entidad no salga del territorio colombiano.
   - El servicio por contratar debe incluir las siguientes capacidades:
     - SOAR
     - Threat Hunting
     - Integración con las plataformas actuales de la entidad en sus medios existentes sean plataformas físicas, servidores o maquinas virtuales.
   - El contratista seleccionado deberá entregar con el servicio las siguientes funcionalidades :
     - Automatización avanzada
     - Analítica avanzada
     - Escalabilidad
     - Uso de tecnologías disruptivas como machine learning, inteligencia artificial, herramientas de visualización, priorización de los eventos basado en el riesgo, gestión de parcheo y remediación y el cumplimiento normativo aplicable a la entidad.
     - Integración con las plataformas actuales de la entidad,
   - El contratista debe implantar en su solución de SOC la logística de atención en sitio requerida para responder a los requerimientos que no puedan ser solucionados en el primer nivel de contacto para mantener, garantizar la disponibilidad del servicio en el menor tiempo posible, dentro de los acuerdos de niveles de servicios requeridos.
   - El servicio de SOC a contratar debe contar con este tipo de tecnologías que facilitan la automatización de los procesos y la información que se está recibiendo entorno a los eventos de seguridad de la información y que faciliten a la entidad la toma de decisiones en tiempo real, y la toma de decisiones en tiempo real, por lo tanto los playbooks, las alertas priorizadas y las acciones automatizadas se definirán entre el contratista y la entidad

durante la prestación del servicio y cuando el SOC entre a operar en su totalidad con el afinamiento de las herramientas y tecnologías que hacen parte del servicio de SOC que incluye: la configuración adecuada de las herramientas de seguridad, la definición de los procedimientos operativos, capacitación del personal de la Entidad, y la adaptación de este servicio con a los riesgos específicos de la Entidad.

- El servicio de SOC debe entregar como mínimo 40 playbooks bien definidos, acorde al análisis de la infraestructura de la entidad y esos playbooks tendrá que se actualizados acorde a las eventualidades encontradas en el desarrollo del contrato.
- Gestionar de manera proactiva los eventos y/o incidentes de seguridad, incluyendo la implementación de medidas correctivas y preventivas para evitar la recurrencia de estos.
- Formular solicitudes ante entidades u organismos del orden nacional, entidades descentralizadas, corporaciones, agencias, autoridades, para la obtención de información requeridas para cumplir con los objetivos del proyecto.
- Realizar análisis, identificación, solución y monitoreo constante de la red, servidores, puntos finales, bases de datos, aplicaciones, aplicaciones web, sitios web y sistemas de información del Datacenter y nube pública de la Aeronáutica Civil, con el fin de identificar y mitigar cualquier actividad sospechosa que pueda indicar un posible incidente de seguridad. (Según anexo técnico)
- Implementar las mejores prácticas en seguridad y normatividad establecidas en la entidad para garantizar una protección adecuada de la información.
- Identificar, analizar, investigar, informar y asistir a la Entidad en la toma de decisiones y conducción de acciones de defensa, de manera oportuna y eficiente a la entidad, sobre cualquier amenaza, vulnerabilidad e incidente de seguridad detectado, cumpliendo con los parámetros establecidos por la entidad y las normativas vigentes en materia de seguridad de la información.

10. El servicio de SOC debe incluir herramientas Análisis Forense Digital, con las siguientes características:
    - El SOC debe utilizar herramientas de análisis forense digital reconocidas y aprobadas para la recolección, análisis y preservación de datos.
    - Dentro del plan de implementación el contratista debe establecer procedimientos estandarizados para la identificación, recolección, análisis e interpretación de datos digitales, asegurando la integridad y validez de la evidencia.
    - El contratista debe asegurar que el personal del SOC se encuentre al día en el estado de arte asegurando que su personal tenga capacitación continua en técnicas avanzadas de análisis forense digital y en el uso de las herramientas mencionadas.

11. El servicio de SOC debe establecer parámetros de preservación de Evidencia Digital, que incluya como mínimo las siguientes actividades:
    - Durante un incidente de seguridad, se seguirán estrictos protocolos para la preservación de la evidencia digital, incluyendo la creación de copias de seguridad inmutables y el uso de técnicas de hash para verificar la integridad de los datos.
    - Se mantendrá una cadena de custodia detallada para todas las evidencias recolectadas, documentando cada acceso y transferencia de datos.
    - La evidencia digital será almacenada en un entorno seguro y controlado, con acceso restringido únicamente al personal autorizado.
    - Después de la resolución del incidente, la evidencia digital será archivada de acuerdo con las políticas de retención de datos de la organización y las regulaciones aplicables.

12. El servicio de SOC debe establecer procedimientos durante y después de un Incidente que incluya como mínimo las siguientes actividades:
    - Se establecerá un equipo de respuesta a incidentes forenses que será activado inmediatamente tras la detección de un incidente de seguridad.
    - Este equipo será responsable de coordinar todas las actividades de análisis forense, asegurando que se sigan los procedimientos establecidos y que se mantenga la integridad de la evidencia.
    - Se generarán informes detallados de todas las actividades forenses realizadas, incluyendo hallazgos, conclusiones y recomendaciones para prevenir futuros incidentes.
    - Se realizarán revisiones post-incidente para evaluar la efectividad de los procedimientos forenses y realizar mejoras continuas.

13. Dentro del servicio contratado (SOC) se debe monitorear los eventos de la infraestructura de seguridad perimetral, la infraestructura de servidores,

y servicios WEB de la Aeronáutica Civil, según especificaciones técnicas del presente documento (formato 8). El contratista de contemplar dentro de ese monitoreo:

- ❖ El monitoreo se debe dimensionar para una cantidad de EPS (eventos por Segundo) mínimo 25,000 eventos diarios y podrá ser redimensionado de acuerdo con las características de las plataformas instaladas por la Aerocivil, y mediante común acuerdo entre el contratista y la entidad.

14. Dentro del servicio contratado (SOC) se debe entregar planes de mejora (incluyendo configuraciones) acorde al monitoreo y realizar el acompañamiento técnico en casos de incidentes de seguridad de los componentes de infraestructura de seguridad con que hoy cuenta la Entidad, según especificaciones técnicas del presente documento (formato 8).

15. Dentro del servicio contratado (SOC) se debe analizar, generar y entregar las configuraciones (incluyendo actualizaciones, parches y remediaciones) de Seguridad a implementar en las plataformas de la Entidad según mejores prácticas del mercado, y acompañar a la Entidad en la correcta implementación de las mismas.

16. Acorde a la evolución de los riesgos de seguridad que se presenten durante la ejecución de contrato. El contratista debe:
    - ❖ Realizar reuniones de seguimiento quincenal, mensual y trimestral dependiendo de la cantidad de eventos presentados y su criticidad previa coordinación con la supervisión del contrato por parte de la Entidad
    - ❖ Analizar la situación de la entidad y entregar las configuraciones de Seguridad y planes de remediación a implementar por la Entidad con la respectiva coordinación a través de la supervisión del contrato.
    - ❖ Para eventos cuya magnitud comprometa de manera crítica la seguridad de la entidad, entre las partes se debe hacer una revisión al momento de la ocurrencia del evento, para determinar pasos a seguir y realizar la remediación en el menor tiempo posible.

17. Dentro del servicio contratado (SOC) se debe detectar posibles amenazas y prestar el apoyo técnico para solucionarlas en el menor tiempo posible.

18. Dentro del servicio contratado (SOC) se debe detectar, analizar, contener y prestar el apoyo técnico para remediar incidentes de seguridad que puedan afectar los sistemas de información y/o infraestructura tecnológica de la Aeronáutica Civil, según especificaciones técnicas del presente documento (formato 8).

19. Dentro del servicio contratado (SOC) se debe prestar el servicio de Threat Hunting para la detección proactiva de amenazas a través de las plataformas integradas desde el SOC con los sistemas de la entidad, y lo que se busca es detectar con anticipación y de manera activa indicios de actividades maliciosas antes de que se manifiesten como ataques evidentes. Para ello el contratista realizará las siguientes actividades por lo menos Dos (2) veces al año durante la prestación del servicio, así:
    - ✓ Comportamientos anómalos en la red, a través de un análisis de vulnerabilidades
    - ✓ Identificación de amenazas avanzadas como APT (Advanced Persistent Threats).
    - ✓ Exfiltración de datos o tráfico sospechoso.
    - ✓ Actividades inusuales en los endpoints.
    - ✓ Inteligencia de Amenazas.

20. El proceso de gestión de incidentes de seguridad del contratista debe estar basado en el Framework, guía y mejores prácticas del NIST 800-53 o ISO 27001 (2013 o superior o 2022), para la creación de los equipos de respuesta ante incidencias de seguridad “CSIRT”. Se validará que el proveedor cuente con certificación ISO 27001 (2013 o superior o 2022).

21. Dentro del servicio contratado (SOC) se debe realizar la gestión de los incidentes detectados, siguiendo las mejores prácticas y normatividad correspondiente, detectando, informado y conteniendo los eventos, llevando registro completo del incidente y reportando al personal designado por el supervisor del contrato.

22. Dentro del servicio contratado (SOC) se debe realizar la gestión de las vulnerabilidades detectadas, informar y entregar las configuraciones (incluyendo actualizaciones, parches y remediaciones) a implementar correspondientes, acompañamiento durante la implementación para la mitigación, y hacer el seguimiento de las vulnerabilidades.

23. Durante la vigencia del contrato, el contratista debe presentar mensualmente propuestas y plan de aplicación de mejoras en la seguridad cibernética mediante las herramientas disponibles en el SOC (casos de uso), la entidad solicita implementar 20 casos durante el primer año, que se aumentarían progresivamente hasta el tiempo contractual en la medida que se entre en operación y se haga toda la armonización de las herramientas integradas con la infraestructura de la ENTIDAD

24. Durante la vigencia del servicio contratado (SOC) se debe realizar seguimiento a la efectividad de los casos de uso.

25. El Contratista debe participar en las ventanas de mantenimiento que la entidad programe, mediante el monitoreo particular de los equipos intervenidos e informando de los eventos detectados durante la ventana.

26. El Contratista debe gestionar, atender y apoyar técnicamente en la solución de los incidentes 7X24X365 y se deberá garantizar una disponibilidad del 99,5 % de los servicios contratados.

27. El Contratista debe asistir a las reuniones presenciales o virtuales que el supervisor del contrato requiera.

28. El Contratista debe contemplar una bolsa de créditos equivalentes a 200 horas que se pueden ser utilizadas por la entidad ~~en~~ durante la vigencia del contrato en:
    - Revisar, analizar, asesorar al personal de la Aeronáutica Civil en las situaciones Post – Incidente.
    - Suministrar información que contribuya a la contención de incidentes.
    - Verificar acciones en la toma de las mejores decisiones a tomar para evitar su ocurrencia futura
    - Servicios post incidente forense como:
        - Preservación de evidencia.
        - Cadena de custodia.

    La distribución de las horas /créditos será determinada por la entidad dependiendo del caso / incidente.

29. En contratista debe incluir dentro del servicio la ejecución de al menos dos (2) programas OJT por año de mínimo 16 horas para transferencia de conocimiento sobre ciberseguridad, de manera virtual sincrónica para 200 funcionarios de la entidad; los temas a cubrir por cada programa serán acordados con la entidad, en todo caso el primero se deberá referir a la etapa de despliegue y puesta en funcionamiento, y las jornadas deben quedar grabadas para que sean accesibles por todo el personal de la entidad de manera asincrónica durante toda la duración del contrato.

30. Los ítems para monitorear dentro del alcance del contrato son:

    - Cantidad de IPs internas, externas y URLs a ser monitoreadas
        - IPs internas 500 escalables a 700 criticas.
        - IPs externas 50 escalable a 128.
        - URLs: 17 escalable a 25.
    - Cantidad de Activos monitoreados SOC: 700 escalable hasta 900
        - Activos críticos: 300 escalable hasta 500
        - Activos Críticos con Agentes Avanzados: 400

- Cantidad de usuarios de alto riesgo para la organización monitoreados SOC:
  - Usuarios Estaciones de Trabajo: 2700 escalable a 3500
  - Usuarios Directorio Activo: 400
  - Usuarios Correo Electrónico O365: 500
- Gestión de Vulnerabilidades:
  - Activos Infraestructura interna: 400 escalable hasta 500
  - Aplicaciones Web: 5
- Cantidad de Activos monitoreados Performance - NOC: 500
  - Activos críticos: 500
- Cantidad de ingesta de logs de seguridad: Dimensionar acorde al detalle en Anexo 1 dentro del documento Formato 8 Especificaciones Técnicas.
- Cantidad de ingesta de telemetría de red: Dimensionar acorde al detalle en Anexo 1 dentro del documento Formato 8 Especificaciones Técnicas.

31. El servicio debe permitir gestionar crecimiento horizontal (nuevos equipos de tecnologías ya instaladas), con un máximo de 10% del número total contratado de activos de TI, durante el periodo de servicio sin costo adicional y crecimiento vertical (nuevas tecnologías) con un máximo de 2 tecnologías anuales (las tecnologías que estamos revisando para crecer son asociadas a infraestructuras de hiperconvergencia, modernización de aplicaciones, bases de datos y funcionamiento en nube), sin costo adicional para Aerocivil.

3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC

32. El Contratista debe contar con herramientas licenciadas (NO CODIGO ABIERTO) que sean compatibles y/o integrables con la plataforma actual de seguridad con que cuenta la entidad para asegurar el funcionamiento de la solución a nivel de interoperabilidad. Adicionalmente las herramientas deben utilizar tecnologías avanzadas de análisis de datos y aprendizaje automático para detectar patrones de comportamiento maliciosos en los sistemas y redes de la Aeronáutica Civil.

33. Todo el software, herramientas, plataformas utilizadas por el Contratista para el monitoreo y funciones propias del SOC, deben estar licenciados y con soporte vigente durante la duración del contrato.

34. Es importante aclarar los instrumentos o herramientas entregadas no podrán implementarse sobre herramientas ofimáticas, sino sobre soluciones tecnológicas estructuradas, como por ejemplo:
    - ❖ Tableros automatizados sobre Inteligencia de negocios, para lo cual, el diseño del instrumento, la configuración, desarrollo e implementación estarán a cargo del contratista y la presentación y resultados finales serían aprobados por la supervisión del contrato.

35. Cabe aclarar que todos los instrumentos o herramientas ofrecidas en el diseño del servicio, el contratista debe entregar a la Aerocivil como parte integral del proyecto, y su disponibilidad será medida acorde a los ANS establecidos.

36. El contratista debe suministrar todos los insumos requeridos por el mismo para el desarrollo del objeto contractual. Incluyendo canal de internet para interconexión, herramientas ofimáticas, pantallas, computadores, software antivirus y herramientas de seguridad.

37. Los componentes tecnológicos de la solución adicionales que provea el Contratista para la prestación de los servicios deben estar debidamente actualizados y soportados por fabrica durante toda la vigencia del contrato.

38. El Contratista debe contar con una herramienta de monitoreo que:
    - ❖ Permita monitorear posibles amenazas de seguridad, como por ejemplo intentos de acceso no autorizados, ataques de denegación de servicio

(DoS/DDoS), ransomware, Phishing, malware, entre otros. Y generen la respectiva alerta a la entidad para ser tratado, como se indica en el presente documento.

- Permita establecer y analizar patrones de comportamiento basados en Usuarios, Entidades, Host y Direcciones IP entre otros.

39. El servicio contratado (SOC) debe tener obligatoriamente una herramienta de integración para administración, escalamiento y gestión de Tickets. Que cumpla con:
    - Debe incluir un módulo para gestión de incidentes de seguridad que permita crear un ticket asignando un número de incidente, clasificando la criticidad automática del evento de acuerdo con el riesgo evaluado, generación de alertas y respuesta ante él (incidente, respuesta).
    - Debe guardar registro de las acciones tomadas por los analistas, los escalamientos y demás actividades en una línea de tiempo específica los cuales permitirán establecer el momento en el que el caso fue cerrado.

40. La Entidad cuenta con el sistema de gestión de tickets (fabricante ARANDA) El proveedor deberá integrar sus sistemas de para administración, escalamiento y gestión de Tickets, con éste, o utilizar ARANDA de manera independiente para gestionar su sistema de escalamiento sin ningún costo adicional hacia la entidad. En este sentido, teniendo en cuenta que el contratista deberá conocer y manejar la herramienta de la entidad (ARANDA), con el fin de asegurar la correcta integración de la misma en el servicio del SOC.

41. El contratista debe contar como mínimo con una herramienta SIEM y las soluciones tecnológicas a utilizar por el contratista para el servicio de SOC, deben ser compatibles y/o integrables con la plataforma actual de seguridad con que cuenta la entidad para asegurar el funcionamiento de la solución a nivel de interoperabilidad.

42. El contratista debe integrar su plataforma SIEM y herramientas de ciberseguridad a utilizar con las plataformas de monitoreo con las que cuenta de la entidad (SolarWinds Platform para monitoreo de canales, para monitoreo de la red tenemos FortiAnalizer y FortiAIOPs, también se encuentra en periodo de pruebas de FortiMonitor, y para correlacionar con sistemas afectados en caso de remediación con el PRTG), la cual debe cumplir las siguientes funcionalidades:

    - Permitir colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la Entidad
    - Debe ser desplegada en un entorno de virtualización y/o hardware que permita garantizar una arquitectura escalable para la Entidad.
    - La plataforma debe integrarse con la solución de Next Generation Firewall con que cuenta la Entidad actualmente, incluyendo todos sus módulos, de manera que se pueda tener una arquitectura integrada e interoperable, donde se pueda tener información consolidada de topología física y lógica, amenazas existentes, y estadísticas de seguridad en general.
    - La plataforma de Security Information and Event Management (SIEM) propuesta debe encuentrarse ubicada en los cuadrantes de las principales empresas de investigación de tecnología, como Gartner y/o Forrester. Específicamente, la solución debe estar catalogada como Líder y/o Challenger en dichos cuadrantes. El oferente deberá adjuntar la calificación y/o certificación correspondiente, que confirme que la solución propuesta se encuentra en las categorías requeridas
    - La solución debe contar con un sistema de bases de datos hibrida, lo que quiere decir que esté basado en NoSQL (BigData) y SQL, no se aceptan soluciones basadas únicamente en motores de bases de datos del tipo SQL, esto con el fin de asegurar que la solución soporte grandes volúmenes de datos sin afectar la estabilidad de la solución.
    - En caso de investigación forense o terminación del servicio el contratista debe entregar los logs comprimidos y cifrados previa coordinación con la supervisión del contrato
    - La solución de SIEM y las herramientas de ciberseguridad a utilizar debe soportar las capacidades de infraestructura que hace parte de este Anexo Técnico.
    - Debe tener la Capacidad de parametrizar métricas definidas por el usuario. Si esto requiere un desarrollo adicional no debe generar costos adicionales a la entidad

- La solución debe soportar las siguientes plataformas a nivel de monitoreo de seguridad y de rendimiento; Antivirus, Application Servers, Authentication Servers, Blade Servers, Cloud Services, Databases, Directory Services, DNS/DHCP Servers, etc., dimensionados según anexo técnico.
- El Contratista debe definir, establecer y asesorar a la Entidad, en la definición de las políticas y parámetros que se configurarán en la solución de SIEM y las herramientas de ciberseguridad a utilizar para la recolección, transporte, agregación, agrupamiento, almacenamiento, respaldo, retención, análisis, correlación, manejo de alertas y visualización, entre otras, de la información relacionada con los eventos que generan y/o almacenan los dispositivos de la Entidad.
- En caso de que el contratista requiera desarrollos adicionales en su plataforma para lograr la integración con las plataformas definidas, el costo esos desarrollos deben ser asumidos dentro del caso de negocio del contratista , sin generar costos adicionales a la entidad.
- Se requiere una plataforma para gestionar de manera unificada, automática y eficiente la operación de seguridad. Para tal fín la solución propuesta debe hacer gestión de los eventos y telemetrías que se generan tanto en la red de área local como en las instancias Cloud. Así mismo debe de estar en capacidad de automatizar tareas más allá de la colección y correlación de eventos proporcionando capacidades de última generación para detección investigación y respuesta ante amenazas (TDIR). La solución debe ser de tipo solución Cloud SaaS que tenga la capacidad de integrarse con tecnologías o entornos On-premise ya existentes en la entidad, permitiendo interoperabilidad con infraestructura local, con etapas de interpretación de datos, priorización y gestión del riesgo y respuesta adaptativa, todos centralizados en un motor de análisis basado en Machine Learning.
- Por lo anterior la solución propuesta debe estar en capacidad de realizar tareas de SIEM de última generación, UEBA, calificación del riesgo y amenazas internas.
- La solución debe incluir la licencia que permita la implementación de casos de uso para detectar ciberamenazas y amenazas internas
- Se debe incluir licenciamiento para análisis de comportamiento de Usuarios y Entidades UEBA
- La retención debe ser 90 días para eventos en caliente (Hot) y 9 meses en frio (Cold), para una retención total de 1 año
- La solución debe ser implementada como Cloud SaaS que tenga la capacidad de integrarse con tecnologías o entornos On-premise ya existentes en la entidad. Para ello se permiten plataformas multimarca, tomando eso en cuenta, todos los módulos requeridos independiente de la marca deben operar de manera unificada.
- La plataforma debe incluir los agentes y/o colectores para la colección de eventos de Windows y Linux, estos agentes deben ser de la misma marca de la solución propuesta.
- Se requiere que la plataforma propuesta permita acceso a la configuración, administración y respaldo de los pipelines por medio de los cuales se conectarán las fuentes de datos.
- Para la gestión de Usuarios de la plataforma, se debe permitir la creación basados en los roles de forma granular y de acuerdo a los privilegios otorgados para los siguientes criterios:
- - Acceso a los tenant: dependiendo del perfil acceso a uno, varios o a todos.
- - Interfaz de Usuario: permitir el acceso de manera selectiva y de acuerdo con el rol con los respectivos privilegios para la creación de Dashboards, Tableros de investigación y gestión de consultas, consola para creación de reglas/ políticas/ modelos/ cadenas de amenaza, configuración de alertas, acciones de respuesta, playbooks y casos.
- - Acceso al menú de configuración general basado en niveles de administración.
- - Configuración de pipelines, creación y manejo de recursos, grupos de recursos, grupos de usuarios, tipos de cuentas, gestión de identidades y fuentes de datos.
- - Archivado y exportación de data, borrado seguro, monitoreo de usuarios de la plataforma y auditoría.
- - Monitoreo y gestión de tenants, agentes y colectores.
- - Permisos de solo lectura.
- La solución debe soportar autenticación SSO basada en LDAP o SAML
- La plataforma propuesta debe permitir enmascaramiento para privacidad de los datos para: Usuarios, Cuentas, Asignaciones, Asignaciones para las cuentas, Roles y Actividades.

- La arquitectura debe permitir multitenancy flexible y escalable de acuerdo con el uso, administrable desde la interfaz de usuario de acuerdo con el rol establecido permitiendo creación y eliminación de instancias sin intervención del area de soporte del fabricante.
- La plataforma propuesta debe estar en capacidad de proveer una arquitectura Cloud SaaS tenga la capacidad de integrarse con tecnologías o entornos On-premise ya existentes en la entidad, permitiendo interoperabilidad con infraestructura local.
- La solución debe contar un Data Lake de "opción abierta" basado en Big Data que permita el acceso y gestión eficiente de datos.
- La solución debe permitir arquitecturas Cloud to Cloud via API y sin necesidad de colectores adicionales.
- La solución debe permitir implementación en nube de ORACLE, AWS, Google y Azure. A la fecha la entidad tiene servicios sobre Azure, y Oracle.
- La solución debe permitir la integración de servicios en la nube:
    - El servicio SOC deberá ser capaz de integrarse de manera efectiva con las principales plataformas de servicios en la nube, incluyendo Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure.
    - Se utilizarán APIs y herramientas nativas de cada plataforma para asegurar una integración fluida y eficiente, permitiendo el monitoreo y la gestión centralizada de la seguridad de los recursos en la nube.
- La plataforma debe recopilar eventos de SIEM existentes o plataformas de almacenamiento de datos/big data como Splunk, Elasticsearch y SnowFlake
- La solución propuesta debe estar en capacidad de hacer descubrimiento de máquinas o activos o permitir la carga manual vía CSV para la creación de listas y grupos para monitoreo.
- La solución debe ser una arquitectura abierta y unificada para cloud y su integración con los puntos ON-premise para todas las funcionalidades incluidas, sin incluir plataformas de terceros y despliegues independientes que vayan en contra de la visión unificada y holística de la operación de seguridad.
- La Solución debe contar con mínimo 500 conectores Out of the Box en total para todas las categorías de las soluciones de la entidad
- La solución debe incluir la capacidad de conectar fuentes custom sin necesidad de aplicar "backend scripting".
- Debe permitir la utilización de datos de eventos de identidad, acceso, CMDB, nube, seguridad y sistema operativo, así como anomalías del tráfico de red, enriquecimiento a partir de conjuntos de datos de inteligencia de amenazas externos para crear un contexto de 360 grados para la detección general de amenazas.
- La solución debe tener capacidades de análisis de tráfico encriptado:
    - El servicio SOC debe contar con herramientas y tecnologías avanzadas para el análisis de tráfico encriptado, tales como soluciones de inspección profunda de paquetes (DPI) y análisis de flujo de tráfico.
    - Estas herramientas deberán ser capaces de identificar y mitigar amenazas en el tráfico encriptado sin necesidad de descifrar el contenido, utilizando técnicas como el análisis de patrones y comportamientos anómalos.
- La solución debe cumplir con preservación de la privacidad:
    - Se implementarán estrictas políticas y procedimientos para asegurar que la privacidad de los datos encriptados no sea comprometida durante el proceso de análisis.
    - El SOC utilizará métodos de análisis que no requieran el acceso al contenido de las comunicaciones encriptadas, garantizando así la confidencialidad de la información.
    - Se mantendrá un registro detallado de todas las actividades de análisis realizadas, asegurando la transparencia y el cumplimiento de las normativas de privacidad aplicables.
- Debe contar con la capacidad de generar diferentes tareas de machine learning basadas en los eventos procesados por el SIEM, y contar con la capacidad de hacer entrenamiento periódico o por demanda de dichos modelos
- Se requiere la ingestión de eventos de actividad de usuarios a través de la integración con el directorio activo, en caso de requerirse agentes estos deben ser de la misma marca de la solución propuesta, no se permiten agentes de terceros.
- La solución debe permitir adicionar casos de uso para: XDR, Network Traffic Analisis e Identity & Access manegement.
- La plataforma debe contar con una librería casos de uso disponibles de acuerdo con el tipo de amenaza o detección, fuente de datos, anomalía y modelos o cadena de amenaza incluyendo análisis de comportamientos y desviaciones sobre líneas base.

- La plataforma debe integrar casos de uso para el monitoreo y la detección en los entornos cloud para: gestión, escalamiento de privilegios, desviaciones en la cantidad de encripciones a nivel de microservicios.
- La plataforma debe permitir detección de ataques de Fuerza bruta por medio de la detección de múltiples intentos fallidos seguidos por un intento exitoso para diferentes criterios de autenticación, creación de perfiles o grupos entre otros ya sea por parte de un atacante o de un usuario interno.
- La plataforma debe incluir detección basada en MITRE ATT&CK, con establecimiento de reglas específicas basadas en diferentes técnicas. Adicionalmente, deberá contar con un Dashboard de MITRE con una vista general que incluya el marcado de eventos o detecciones que coincidan con cada una de las técnicas
- La herramienta debe permitir la creación de dahsboard granulares y personalizados con gráficas y listas, así como de reportes a partir de un dashboard específico.
- De igual manera, debe incluir herramientas de análisis gráfico de los eventos a partir de una consulta por medio de un menú gráfico y sin necesidad de generar un query. Los gráficos deben incluir diagramas de barras, con multiples TABS, tipo burbuja, pie, red entre otros.
- Debe contar con la posibilidad de personalizar las columnas con los campos en la visualización de los eventos de acuerdo a los atributos en forma tabular y sin necesidad de usar un query para tal fin.

HERRAMIENTA SOAR

- La herramienta SOAR debe comportarse como una solución que incorpore automatización avanzada, analítica avanzada, escalabilidad, uso de tecnologías disruptivas como machine learning, inteligencia artificial, herramientas de visualización y el cumplimiento normativo aplicable a la entidad. Debe contar con Integración con las plataformas actuales de la entidad. El servicio de SOC a contratar debe contar con este tipo de tecnologías que facilitan la automatización de los procesos y la información que se está recibiendo entorno a los eventos de seguridad de la información y que faciliten a la entidad la toma de decisiones en tiempo real, por lo tanto los playbooks, las alertas priorizadas y las acciones automatizadas se definirán entre el contratista y la entidad durante la prestación del servicio y cuando el SOC entre a operar en su totalidad con el afinamiento de las herramientas y tecnologías que hacen parte del servicio de SOC que incluye: la configuración adecuada de las herramientas de seguridad, la definición de los procedimientos operativos, capacitación del personal de la Entidad, y la adaptación de este servicio con a los riesgos específicos de la Entidad.
- Debe contar con playbook de respuesta a incidentes prediseñados. Esto, para minimizar la necesidad de desarrollo personalizado y ahorro de tiempo y recursos
- Debe tener la capacidad de gestionar los casos de uso (mínimo tres) y permitir al administrador de la plataforma dimensionarlos en la medida en que la entidad en conjunto con el contratista va encontrando posibles superficies de ataque a proteger
- Debe permitir creación de playbooks definidos por usuario o definidos por template
- Debe tener la capacidad de realizar un seguimiento de las investigaciones de incidentes, los procedimientos y la información complementaria para alertas de amenazas y eventos de riesgo.
- Debe permitir integración con los principales fabricantes de SIEM, y en general con los principales fabricantes de Ciberseguridad en el mercado, incluida la plataforma de Ciberseguridad en la entidad
- Debe tener la capacidad de analizar, investigar y responder a incidentes usando tecnologías de Inteligencia Artificial

SOLUCIÓN DE PROTECCIÓN DE MARCA

- El contratista deberá proveer el servicio de protección de un (1) dominio marca y tres (3) subdominios de marca. Entregar reporte de exposición de amenazas externas. Las palabras clave serán acordadas según análisis preliminar. El reporte deberá incluir
  - ✓ Exposición ante Amenazas en la Dark web
  - ✓ Exposición ante Amenazas en la Surface Web
  - ✓ Exposición ante Amenazas en la Deep web
  - ✓ Menciones en grupos de crimen y foros de ciberdelincuentes.

- ✓ Descubrimiento de forma proactiva de fugas de datos, campañas de phishing y otras amenazas online dirigidas contra su organización.

- ❖ El servicio ofertado para el monitoreo de actividad anómala de Phishing, aplicaciones móviles falsas, registro de dominios similares, malvertising, suplantación de identidad ejecutiva, uso inapropiado y suplantación de marca, suplantación de perfiles sociales, violación de derechos de autor, robo de propiedad intelectual, falsificación de correo electrónico del dominio original.
- ❖ El servicio debe ser en modalidad 7x24 y en tiempo real para identificar de manera oportuna, alertar y derribar los ataques identificados, así como patrones y comportamientos sospechosos.
- ❖ El servicio debe cubrir todo el ciclo de vida de una alerta, desde que se inicia hasta que se soluciona, permitiendo a la institución/compañía tener completo conocimiento de la gestión de cada incidente mediante la consola de administración de la solución así como por medio de alertas mediante correo electrónico.
- ❖ El servicio tendrá la capacidad de consumir y procesar los Weblogs de los portales monitoreados con el objetivo de realizar detección de incidentes de fraude.
- ❖ El contratista debe asignar a la cuenta un ingeniero certificado por el fabricante del servicio, encargado de entregar el estatus del servicio, actualización del alcance, inclusión y/o remoción de palabras claves, definir canales de comunicación, validar la periodicidad de los reportes desde el portal del servicio, entre otros. El especialista debe estar en el mismo huso horario, en la misma región, hablar español nativo, y tener disponibilidad para atender cualquier inquietud del cliente.
- ❖ El servicio deberá incluir la detección y desactivación de perfiles y/o cuentas falsas en redes sociales que suplanten la identidad de la institución/compañía.
- ❖ El servicio deberá incluir la detección y desactivación de perfiles y/o cuentas falsas en redes sociales que suplanten la identidad de los funcionarios de alto rango, de la institución/compañía, siempre y cuando dichos perfiles estén siendo usados para engañar a los usuarios o propagar fraude.
- ❖ Protección contra Aplicaciones Móviles No Autorizadas, que estén siendo atacadas para robar datos de clientes o para instalar malware, mediante el uso indebido de la marca y/o el nombre de la institución/compañía. Por lo tanto, se debe contar con un servicio de identificación y remoción de esas aplicaciones.
- ❖ La consola de administración para el surface, puede ser en idioma español o inglés. Así como el soporte y sus diferentes canales de comunicación, tales como, correo electrónico, contactos telefónicos.
- ❖ El servicio de monitoreo deberá notificar alertas a través de diversos canales de comunicación, tales como, correo electrónico, portal de administración, entre otros.
- ❖ El servicio deberá estar en la capacidad cuando sea viable técnicamente de identificar si los usuarios víctimas de sitios fraudulentos detectados ingresaron información y de ser posible obtener la información que ingresaron.
- ❖ La solución debe poder gestionar de forma inteligente casos de intento de ingreso a la entidad con información obtenida por phishing, poder identificar los usuarios que entran, cuantas veces ingresan, desde que dirección IP, su geolocalización, entre otros, mostrando la evidencia.
- ❖ Contar con fuentes internas de proactividad, como es el caso de las búsquedas automatizadas haciendo uso de las capacidades de las herramientas de aprendizaje con las que cuenta el servicio.
- ❖ El servicio debe tener la capacidad de recibir los correos electrónicos de los usuarios (abuse boxes), procesarlos para detectar posibles casos de fraude. Este servicio puede entregarse como un caso de uso.
- ❖ El servicio deberá contar con funcionalidades de machine learning para analizar la probabilidad de que las URL´s sean phishing.
- ❖ Es requerido que fabricante del servicio, pertenezca a un grupo de la industria de referencia a nivel global en términos de protección antiphishing.
- ❖ El fabricante directamente debe ofrecer acompañamiento de por lo menos una persona especializada a lo largo del servicio que pueda entregarle periódicamente informes adicionales, resumen de lo encontrado con el servicio y estadísticas, actualización del servicio: modificación de keywords, dominios, marcas, entre otros.

43. El servicio contratado (SOC) debe ser gestionado por tableros de control (Dashboards) y el contratista debe asegurar acceso de revisión, lectura y extracción de información a la Entidad durante la vigencia del contrato.

44. El contratista debe crear, configurar y personalizar los tableros de control (Dashboard), recomendados por las mejores prácticas para garantizar el correcto seguimiento a los eventos generados en la plataforma tecnológica definida por la entidad en donde:
    - ❖ Dashboards de visualización en donde se visualicen eventos, incidentes, capacidad, y las estadísticas que sean de interés para la operación del SOC y la entidad
    - ❖ Dashboard de Gestión en donde se proporcione información global en tiempo real sobre un cuadro de mandos, que incluya:
        - El estado de los servicios (incluyendo los cumplimientos de los ANS's comprometidos)
        - El estado de los eventos sobre con la información detallada y los analistas del SOC asignados al evento.
        - El estado del monitoreo del evento y las acciones ejecutadas por los analistas del SOC
        - Una presentación gráfica de la funcionalidad de los servicios monitoreados.
        - Comportamiento de la red de monitoreada de la entidad.

45. El contratista debe entregar acceso de visualización y edición de todos los dashboard diseñados al coordinador y supervisor del contrato. En donde el coordinador y el supervisor puedan tener las siguientes facilidades:
    - ❖ Capacitar 3 funcionarios (incluyendo al supervisor) en poder personalizar las visualizaciones de los dashboards.
    - ❖ Incluir a usuarios adicionales y asignar roles acordes a las necesidades de visualización de eventos requerida por la Entidad

46. El contratista debe asegurar que el Dashboard de Gestión cumpla con las siguientes funcionalidades:

    - ❖ El Dashboard debe ser visible en línea de forma segura a través de un acceso web seguro con doble factor de autenticación.
    - ❖ El Dashboard debe permitir gestionar los incidentes usando un número de ticket, además este debe contar con la información relevante del incidente para revisión de la Entidad.
    - ❖ El Dashboard debe realizar un seguimiento de la prestación del servicio actualizados, presentando el cumplimiento de los ANS's de forma periódica como lo son "Tiempo de respuesta inicial", "Fecha de apertura de ticket", "Prioridad", "Estado" y "Tiempo total de solución".
    - ❖ El Dashboard debe permitir realizar configuraciones de vistas resumidas que puedan ser personalizables.
    - ❖ El Dashboard debe contar con vistas de acuerdo con los roles necesarios para los diferentes niveles que indique la Entidad.

47. Mediante el uso de las herramientas del SOC, el contratista debe:
    - ❖ Crear las alarmas, de acuerdo con los niveles de criticidad establecidos por las mejores prácticas y normatividad de la entidad, enviando las notificaciones vía gráfica, correo electrónico u otro mecanismo de comunicación.
    - ❖ Debe suministrar datos en tiempo real con datos de identidad, información de activos, inteligencia de amenazas y datos de tablas de búsqueda.

48. El contratista a través del SOC debe contar con capacidades de Inteligencia de Ciberamenazas en forma de:
    - ❖ Feeds de Indicadores de Compromiso (IoC) de múltiples fuentes.
    - ❖ Las fuentes de inteligencia de amenazas deben incluir proveedores comerciales, fuentes de código abierto, y colaboraciones con la comunidad de ciberseguridad, asegurando una cobertura amplia y actualizada de las amenazas emergentes.
    - ❖ El SOC implementará una plataforma centralizada para la agregación y gestión de feeds de inteligencia de amenazas, permitiendo la correlación y análisis de datos de múltiples fuentes, Se establecerán procedimientos para la actualización continua y automática de los feeds de IoC, garantizando que el SOC disponga de la información más reciente y relevante sobre amenazas

49. El contratista y el servicio contratado de SOC debe cumplir a cabalidad con la normatividad vigente de protección de datos personales.
    - ❖ En caso que por efectos de la presentación del servicio el Contratista requiere acceder, recolectar, almacenar, procesar, respaldar y usar

información de carácter personal de los titulares de la Entidad, el Contratista debe demostrar que cuenta con una política interna de Protección de Datos Personales que cumpla con los requisitos previstos en el régimen de protección de datos personales.

50. El Contratista debe alinearse al cumplimiento de las siguientes normativas durante la ejecución del contrato:
    - ❖ Decreto 338 – Marco Seguridad Digital para Entidades Publicas
    - ❖ ISO/IEC 27001 – Gestión SegurInfo (114 Controles – 14 Dominios)
    - ❖ ISO/IEC 27032 – Intercambio de información / Manejo de incidentes.
    - ❖ NIST SP 800-39 – Gestión de Riesgos SeguInfo
    - ❖ CSF – NIST
    - ❖ CRF (Coomon Regulatory Framework on Cybersec (Gestion de Riesgos)
    - ❖ Ley 1581 – Protección de Datos Personales

51. El Contratista seleccionado debe presentar a la Entidad antes del inicio de la ejecución del contrato un estudio de seguridad para todo el personal que hará parte del servicio de SOC de menos de 3 meses de anterioridad al inicio del contrato con el fin de que los profesionales encargados de monitorear, detectar, y responder a incidentes de ciberseguridad de la Aerocivil, cuenten con las credenciales, confiabilidad y experiencia necesarias para proteger los activos críticos de información de la Entidad. Para ello se debe realizar el correspondiente estudio de seguridad a través de una Entidad acreditada en la realización de estos estudios, el estudio debe tener mínimo los siguientes elementos:
    - ✓ Revisión de antecedentes Penales
    - ✓ Verificación de Antecedentes Judiciales y Disciplinarios
    - ✓ Evaluación de Riesgos por Conflictos de Intereses
    - ✓ Evaluaciones técnicas de credibilidad y confiabilidad (Poligrafía)
    - ✓ Compromiso con la Confidencialidad
    - ✓ Análisis de redes sociales.

52. Todas las herramientas dentro del servicio de SOC deben tener una disponibilidad de 24 x 7 x 365 y el contratista debe garantizar una disponibilidad del 99,5 % de las mismas.

3.1.3 Plan de comunicaciones

53. El contratista como uno de los primeros entregables debe presentar un plan de comunicaciones para asegurar la adecuada prestación de los servicios del SOC, con esquema de niveles y roles que aseguren los acuerdos de niveles de servicios.

54. El plan de comunicaciones del Contratista debe cumplir con:

    - El servicio de atención en el idioma español, para la interacción de las áreas de operación.
    - Ser entregado durante los primeros diez (10) días de ejecución del contrato debe presentar para aprobación del supervisor
    - Debe incluir el plan de entrega de los diversos informes a ser presentados y los tableros de monitoreo y control a ser implementados en desarrollo del objeto del contrato.
    - El plan debe incorporar una matriz de responsabilidades para cada uno de los servicios a desarrollar.

55. El plan de comunicaciones del Contratista incluir como obligación los siguientes items:
    - Puntos de contacto: El contratista debe designar a una persona o equipo de personas como puntos de contacto para la entidad. Estos puntos de contacto deben estar disponibles 7X24X365 para responder a cualquier pregunta o inquietud del supervisor del contrato.

- Horarios de atención: El contratista debe establecer horarios de atención claros y precisos para el personal de la entidad, de modo que la comunicación sea eficiente y efectiva; dando cumplimiento a la disponibilidad 7x24x365 para responder a cualquier pregunta o inquietud del supervisor del contrato o a quien el designe.
- Protocolos de comunicación: El contratista debe establecer protocolos claros para la comunicación entre el Contratista y la entidad. Esto debe incluir la frecuencia y el formato de los informes de seguridad, la forma en que se notificarán los incidentes de seguridad y la forma en que se comunicarán las actualizaciones y mejoras del servicio.
- Canales de comunicación: El contratista debe establecer canales de comunicación adecuados para la entidad. Esto podráincluir correo electrónico, chat, videoconferencia, teléfono u otros medios de comunicación.
- Reuniones de seguimiento: El contratista debe disponer de espacios como mínimo para 1 reunión mensual de seguimiento para verificar el avance de los servicios prestados, mejoras y analizar situaciones presentadas durante el desarrollo de la ejecución del contrato.

3.1.4 Obligaciones sobre Informes y políticas que el contratista debe cumplir.

56. El contratista debe cumplir con el siguiente esquema de entregables de información:

- Reportes semanales sobre el estado y salud de las plataformas existentes.
- Informes quincenales de eventos de seguridad.
- Informes de cumplimiento de los ANS establecidos a nivel mensual.
- Dashboard del servicio en línea propio que concentre toda la información solicitada en el servicio del SOC.
- Informes mensuales de eventos de comportamiento anómalos.
- Informes por demanda acorde con una situación específica o resultado de actas de seguimiento, planes de acción,cronogramas, correos electrónicos o comunicaciones oficiales.
- Informes mensuales de las actividades realizadas objeto de la prestación del servicio del SOC.

57. El contratista debe proporcionar informes de seguridad regulares y detallados que permitan a la entidad evaluar la efectividad y calidad del servicio prestado. Y estos informes deben cumplir:

- Los informes de seguimiento se deben presentar dentro de los cinco primeros (5) días hábiles de cada mes, hasta la liquidación del contrato.

- Los informes deben presentar información de una forma clara y concisa y deben permitir realizar un seguimiento detallado de la ejecución del proyecto.

- El contratista debe seguir las recomendaciones de presentación de estos establecidas por la supervisión del contrato. Así mismo y de ser necesario, se debe incluir información adicional solicitada por la Institución a través del Supervisor del contrato.

- Los informes de seguimiento mensual deben incluir como mínimo:

  - ✓ Resumen ejecutivo.
  - ✓ Actividades realizadas.
  - ✓ Informe por actividades respecto a las obligaciones.
  - ✓ Seguimiento al Cronograma.
  - ✓ Avance de ejecución presupuestal.
  - ✓ Dificultades encontradas durante la ejecución del proyecto
  - ✓ Gestión de Riesgos del proyecto.

- ✓ Recomendaciones relacionadas con la gerencia y ejecución del proyecto.
- ✓ Avance del proyecto.

NOTA: Entiéndase Avance del proyecto como la identificación de cada actividad del servicio, incluyendo la duración programada, la duración remanente, las fechas de inicio y de finalización, programada y reales de ejecución de cada actividad.

58. Dentro del proceso de seguimiento el SOC debe realizar auditorias regulares, que cumplan con los siguientes puntos:
    - ❖ Requisitos de Auditoría:
        - El SOC alquilado deberá someterse a auditorías regulares para asegurar el cumplimiento con las normativas y estándares de seguridad aplicables.
        - Las auditorías serán realizadas por entidades independientes y certificadas, garantizando la objetividad y la integridad del proceso de auditoría.
    - ❖ Frecuencia de las Auditorías:
        - Las auditorías se llevarán a cabo al menos una vez al año, o con mayor frecuencia si así lo requieren las normativas específicas o las políticas de la organización.
        - Se podrán realizar auditorías adicionales en respuesta a incidentes de seguridad significativos o cambios importantes en la infraestructura del SOC.
    - ❖ Alcance de las Auditorías:
        - Las auditorías cubrirán todos los aspectos relevantes del SOC, incluyendo la gestión de datos, la seguridad de la infraestructura, los procedimientos de respuesta a incidentes y la preservación de la privacidad.
        - Se evaluará el cumplimiento con los requisitos específicos de estándares de seguridad aplicables como ISO/IEC 27001.
    - ❖ Informes y Acciones Correctivas:
        - Tras cada auditoría, se generará un informe detallado que incluirá los hallazgos, las áreas de mejora y las recomendaciones para asegurar el cumplimiento continuo con las normativas y estándares de seguridad.
        - El SOC deberá implementar las acciones correctivas necesarias para abordar cualquier deficiencia identificada durante la auditoría, y se realizará un seguimiento para verificar la efectividad de dichas acciones.
    - ❖ Transparencia y Colaboración:
        - Los resultados de las auditorías serán compartidos con las partes interesadas relevantes, incluyendo la alta dirección y los equipos de cumplimiento de la organización.
        - Se mantendrá una colaboración constante con los auditores y las autoridades reguladoras para asegurar que el SOC esté siempre alineado con las mejores prácticas y los requisitos legales.

59. El contratista debe garantizar la confidencialidad de la información recopilada, asegurando que no será utilizada para fines diferentes a los indicados por la entidad, y que no será expuesta o compartida con ninguna otra persona, entidad u organización, sin la autorización expresa de la Aeronáutica Civil.

60. El contratista debe establecer claramente dentro de un documento la estructura para reportar los incidentes de seguridad y los procesos para su respectiva mitigación.

61. En caso de requerirse, el supervisor del contrato debe tener acceso en cualquier momento a los documentos, informes, tableros de monitoreo y control, al igual que a los informes sobre el estado de las categorías o bloques de servicios (con sus correspondientes agregaciones o desagregaciones) definidos.

62. El contratista debe proporcionar la información que le permita a la Entidad fortalecer los siguientes procesos dentro del alcance de sus labores dentro del

contrato:

- Puesta a punto y auditoria del servicio de monitoreo y alertamiento.
- Eliminación segura de la información que ya no se requiera.
- Gestión y Respuesta a incidentes.
- Priorización de incidentes.
- Detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad.
- Priorización de atención de incidentes.
- Atención y escalamiento de requerimientos.
- Mejora Continua del servicio.
- Gestión de cambio sobre la plataforma que soporta el servicio.
- Controles de acceso a los repositorios de información necesarios para la Aerocivil gestionados, y así evitar el acceso no autorizado.
- Modelo de Seguridad predictiva.

63. El contratista debe presentar un informe detallado de causas y acciones de las incidencias de ciberseguridad detectadas con plan de acciones a tomar por la entidad para evitar a futuro, este informe se entregará cada 15 días con los incidentes y remediaciones que se presenten en este tiempo Adicionalmente para eventos cuya magnitud comprometa de manera crítica la seguridad, debe hacerse una revisión al momento de la ocurrencia del evento, para determinar pasos a seguir y realizar la remediación en el menor tiempo posible.

64. El contratista debe entregar a la entidad un informe resumido cada 6 meses, para que la Entidad lo utilice para la actualización del procedimiento, manual o instructivo de seguridad de la información implementado por la Aeronáutica Civil.

65. El contratista debe crear reportes e informes personalizados que permitan a la supervisión del contrato determinar claramente las falencias presentes en los dispositivos, aplicaciones y servicios monitoreados, los cuales podrán ser generados en las escalas de minutos, horas, días, meses y años.

66. Los reportes e informes deben poderse descargar generar en cualquier momento, o cuando el supervisor del contrato, o quien este designe, lo requiera, en formato PDF, HTML, CSV, XLS o el indicado por el supervisor del contrato.

67. Los reportes e informes que incluyan firmas deben entregarse en pdf.

68. En cualquier momento de la ejecución del proyecto y en consenso con el contratista, la Institución podrá solicitar informes específicos de aspectos técnicos, administrativos, financieros y demás aspectos relacionados con la ejecución del proyecto, los cuales deben ser entregados en un término no mayor a diez (10) días calendario o en su defecto en el término definido por la Entidad Contratante dependiendo el tipo de información solicitada.

69. El tiempo de retención de logs de incidentes de seguridad son:
    - 90 días para eventos en caliente (Hot)
    - 9 meses en frio (Cold)
    - Retención del historial total por 1 año (90 días(3 meses) + 9 meses =12 meses)

70. El Contratista debe estructurar los procedimientos y documentos para llevar el control, responsables y niveles de escalamiento, al igual que configuración de las alarmas de eventos de acuerdo con la criticidad que la entidad determine, emitiendo las notificaciones correspondientes al personal que indique el supervisor del contrato, incluidos los posibles canales como: víagráfica, correo electrónico, mensaje de texto u otros.

71. El contratista debe contar con procesos y procedimientos de gestión de incidentes que deben integrarse a los procedimientos con lo que la entidad actualmente se encuentra operando. El contratista basado en su experiencia podrá recomendar el mejoramiento de los procesos actuales de la Entidad, mediante configuraciones a aplicar sobre los equipos de la entidad y acompañar a la entidad a su respectiva aplicación.

72. Al final del contrato el Contratista debe presentar un informe final de los servicios prestados de SOC con toda la información detallada y los soportes respectivos de cada servicio, éste debe ser aprobado por parte del Supervisor designado por la Institución. Debe contener información consolidada de las principales etapas del proyecto, información histórica sobre la ejecución del proyecto, las lecciones aprendidas, principales casos de éxito y las principales dificultades encontradas durante la ejecución del contrato y las configuraciones recomendadas para mitigar las mismas.

73. Los procesos de gestión y operación del SOC deben estar basados con las mejores prácticas establecidas por el modelo de procesos ITIL v4

74. La supervisión en consenso con el contratista, podrá solicitar información adicional a la señalada anteriormente, así como recomendar medidas para mejorar los resultados y en caso de ser aceptadas, el contratista implementará dichas recomendaciones.

3.1.5 Obligaciones sobre el equipo de trabajo que el contratista debe proveer.

75. El contratista debe disponer de personal técnico cualificado para llevar a cabo la ejecución del contrato, conforme los requerimientos exigidos por la entidad, así como aquellos que el contratista considere necesarios para la entrega a satisfacción de los servicios adquiridos dentro del alcance del SOC.

76. El equipo que componga el servicio contratado (SOC) debe contar con un grupo interno con especialidad en atención de incidentes de seguridad.

77. El personal técnico del contratista adjudicatario para proveer el servicio del SOC debe cumplir con los requerimientos y documentación solicitada por la entidad en el documento de especificaciones técnica Formato 8.

78. El equipo del contratista adjudicatario debe componerse como mínimo por los siguientes roles y cantidades de personas que deben estar presentes durante la duración de la ejecución del contrato:

RECURSO	FORMACIÓN	POSTGRADO	CERTIFICACIONES	EXPERIENCIA	DEDICACIÓN	FUNCIONES GENERALES

UN (1) GERENTE DEL SOC.	Ingeniería electrónica o telemática o de sistemas o telecomunicaciones o afines, entendidascomo aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.	En Maestría y/o especialización en Ciberseguridad y Ciberdefensa o Gestión de Proyectos de Ingeniería o Seguridad de la información o Gerencia de sistemas de información o Gerencia de Proyectos de Telecomunicaciones o Gerencia de proyectos o afines.	Certificación PMP y/o Scrum Foundation Professional Certificate (SFPC) y/o Itil V4	Mínimo cuatro (4) años de experiencia laboral desarrollando actividades como gerente, líder o coordinador técnico de proyectos de TI y/o liderando proyectos de Ciberseguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	20 % al proyecto, de requerirse demanera presencial o virtual en las instalaciones de la entidad	Debe encargarse de la gerencia de proyecto, documentación, organización y coordinación de actividades con la entidad.
DOS (2) ANALISTASDE SEGURIDAD	Ingeniería electrónica o telemática o de sistemas o telecomunicacioneso afines, entendidascomo aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.	N/A	Certificación vigente en seguridad en redes y/o especialidad en seguridad operativa, emitida por el fabricante de las soluciones de SIEM, SOAR y/o Protección de marca, CHFI o CIHE, Auditor líder o interno ISO 27001:2022 o 2013 o superiores	Mínimo cuatro (4) años de experiencia laboral desarrollando actividades en seguridad informática. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	50 % al proyecto, de requerirse demanera presencial o virtual en las instalaciones de la entidad	Monitorear y analizar los sistemas de seguridad de la Institución, y tomar medidas para proteger los datos y recursos contra las amenazas de seguridad.

UN (1) COORDINADOR DEL EQUIPO SOC	Ingeniería electrónica o telemática o de sistemas o telecomunicaciones o afines, entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.	N/A	Certificación vigente en seguridad de redes y análisis de vulnerabilidades y/o superficies de ataque, Como, por ejemplo Certificación de Auditor Interno ISO/IEC 27001: 2022 o 2013 o superiores y CIH ó CIHE (Certified Incident Handling Engineer).	Mínimo dos (2) años de experiencia laboral desarrollando actividades relacionadas con coordinación de equipo SOC. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	100% al proyecto	. Liderar y coordinar el equipo de respuesta a incidentes tipo SOC durante todo el proceso de gestión de incidentes. Identificar y clasificar los incidentes de seguridad informática según su gravedad y riesgo para la organización. Evaluación y análisis exhaustivo de los incidentes de seguridad informática para determinar su origen, su alcance y su impacto en la Institución Presentar informes contra medidas de contención para evitar que el incidente se propague y cause más daño a la Institución. Apoyar con

						otras Dependencias, para asegurar una respuesta integral y efectiva ante los incidentes. Elaborar informes y documentación detallados sobre los incidentes de seguridad informática y las acciones tomadas para su resolución. Revisar y apoyar la actualización regularmente el plan de respuesta a incidentes para garantizar que la organización esté preparada para enfrentar futuros incidentes
DOS (2) ANALISTAS DE VULNERABILIDADES	Ingeniería electrónica o telemática o de sistemas o telecomunicacioneso industrial o afines, entendidas como aquellas que comparten núcleo básico de conocimiento, de	N/A	Certificación vigenteen análisis de vulnerabilidades y/osuperficies de ataque, emitida por el fabricante de la marca ofertada.	Mínimo Dos (2) años de experiencia laboral desarrollando actividades como ANALISTA DE SEGURIDAD y/o VULNERABILIDADES. La experiencia se cuenta a partir de la	50 % al proyecto, de requerirse demanera presencial o virtual en las instalaciones de la entidad	(Monitorear constantemente las alertas de seguridad y los registros de eventos para identificar cualquier actividad

	acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional.			expedición de la tarjeta profesional.		sospechosa en la red o en los sistemas de la Institución. Si se detecta una amenaza o un incidente de seguridad, el analista debe investigar y analizar los registros de eventos para identificar la causa del incidente y su alcance. Proponer medidas de mitigación: El analista debe proponer medidas de mitigación y soluciones para prevenir futuros incidentes y reducir los riesgos. Comunicar los resultados: El analista debe comunicar los resultados de su investigación y análisis a otros miembros del equipo de seguridad de la Institución. Debe mantenerse

						actualizado con las últimas amenazas y técnicas de ataque y estar familiarizado con las herramientas de seguridad y los procedimientos necesarios para combatirlas.

**NOTA: Por lo menos uno de los perfiles presentados debe contar con una (1) certificación en soluciones de ciberseguridad de Fortinet.

79. Para evaluar el equipo que estarán involucrados en el contrato el contratista adjudicatario debe entregar los siguientes documentos por las personas que compongan el equipo a evaluar:

Carta de intención	Suscrita por el contratista.
Título profesional	Copia del Diploma o Acta de Grado o Título Profesional, expedido por la respectivaUniversidad; acreditado según la legislación de cada estado. Los títulos de educación superior otorgados por instituciones extranjeras deben presentarse convalidados por el Ministerio de Educación Nacional.
Matrícula profesional	Copia de la matricula o tarjeta profesional para profesionales colombianos, según la normatividad legal aplicable.
Certificado vigencia de la matrícula profesional	Certificado de la vigencia de la matricula profesional o equivalente, vigente a la fecha de cierre del presente proceso, para profesionales colombianos para la evaluación de los roles a presentar con la propuesta.
Título posgrado	Copia del Diploma o Acta de Grado, expedido por la respectiva Universidad o Institución de Educación, debidamente acreditada conforme a la legislación de cada Estado. Los títulos otorgados por instituciones extranjeras deben presentarse convalidados por elMinisterio de Educación Nacional.
Certificaciones	Copia de las certificaciones obtenidas y exigidas como formación académica según el ROL a desempeñar, debidamente expedidas por las organizaciones o instituciones autorizadas.
	Certificaciones de experiencia expedidas por la entidad o la empresa contratante en las que se indique: ● Cargo ● Tiempo Laborado ● Objeto u Objetivo del cargo ● Contratante ● Contacto
Documento de identificación	Ejemplar legible de la cédula de ciudadanía, cédula de extranjería o pasaporte.

Permiso temporal para ejercersin matrícula a personas tituladas y domiciliadas en el exterior	Los profesionales extranjeros deben presentar el correspondiente permiso temporal para ejercer sin matrícula profesional, a la suscripción del acta de inicio.

Notas:

- El adjudicatario **debe entregar antes de la firma del acta de inicio debe allegar el formato de hoja de vida y las hojas de vida con los debidos soportes del personal a contratar** para realizar la suscripción del contrato, so pena de hacer efectiva la póliza de cumplimiento.
- La aprobación de las hojas de vida será realizada por el supervisor del contrato.
- Un mismo profesional no puede ser ofrecido para dos o más cargos diferentes.
- Las certificaciones de experiencia de los profesionales deben ser expedidas por la persona natural o jurídica con quien se haya establecido la relación laboral o de prestación de servicios.
- El Contratista es responsable de verificar que los profesionales propuestos tienen la disponibilidad real para la cual se vinculan al proyecto.
- El personal calificado será el que realice las actividades contratadas, y por lo tanto los informes deben estar suscritos y avalados por los responsables de cada actividad funcional.
- El equipo de trabajo mínimo solicitado se requiere sin perjuicio de que el contratista disponga de un recurso humano adicional para la ejecución del contrato.
- En todo caso la Entidad se reserva el derecho de verificar la documentación presentada.
- Para la correcta ejecución del contrato se debe tener en cuenta lo siguiente: Control del personal y del equipo del contratista

NOTA 1: Se verificará que el personal ofrecido en la oferta del contrato sea el necesario e idóneo para la ejecución de las actividades, que permitan el cumplimiento integral del objeto contractual.

NOTA 2: El Contratista se obliga a cancelar al personal ofrecido en su oferta, el salario y prestaciones sociales estipuladas en la normatividad vigente, así como pagar los aportes sistema de seguridad social integral con base en dicho salario, conforme a los valores de la oferta presentada y debe mantener indemne a la Institución de cualquier acción o reclamación por este concepto, teniendo en cuenta que no se genera ningún tipo de vínculo contractual o laboral entre el personal de Consultoría y la Institución.

NOTA 3: En la medida en que se incorporen los diferentes profesionales y especialistas, se debe programar una reunión entre dichos profesionales o especialistas aprobados y la supervisión del contrato, para coordinar y tratar el desarrollo de los respectivos aspectos técnicos del proyecto a ejecutar. De esta reunión se debe elaborar la correspondiente acta.

80. El contratista debe asumir el costo de la carnetización de todo el personal que vincule para el cumplimiento del contrato, conforme al procedimiento que le señale la Aerocivil. La Aerocivil dará la información sobre el precio de este servicio.

Nota: Todas las características técnicas descritas en el presente formato 8 son de obligatorio cumplimiento para el contratista.

3.2 DETALLES DEL DESARROLLO DEL CONTRATO

3.2.1 Fases del contrato

- Transición, Recepción y verificación de la infraestructura tecnológica: En esta fase se verificará por parte del contratista toda la infraestructura

tecnológica que será integrada al servicio del SOC.

- Planificación: En esta fase se establecerá un plan de trabajo por parte del contratista y se definirá la estrategia a seguir para la implementación del servicio de SOC.
- Configuración y despliegue: El contratista configurará y desplegará el servicio de SOC, incluyendo la instalación de hardware y/o softwares necesarios para la monitorización y análisis de la red y los sistemas.
- Integración con otros sistemas: El contratista integrará el servicio de SOC con los sistemas existentes a nivel de seguridad con los que cuenta la Aerocivil y hará esta integración con los sistemas de gestión de eventos de seguridad (SIEM) y las demás herramientas que se vayan a implementar dentro del alcance de los servicios del SOC.
- Pruebas de validación: Se llevarán a cabo pruebas de validación para verificar que el servicio de SOC esté funcionando correctamente y cumpliendo con los objetivos establecidos.
- Entrenamiento: El contratista proporcionará entrenamiento especializado al personal de la Aerocivil que utilizará el servicio de SOC, para asegurar que estén familiarizados con el uso del sistema y puedan responder eficazmente a las alertas y eventos de seguridad. Se deben impartir Dos (2) entrenamientos por año para el personal de infraestructura y seguridad de la secretaria de TI, que serán independientes al entrenamiento inicial de funcionamiento y administración de la plataforma de seguridad integrada por el contratista.
- Mantenimiento y actualizaciones: El contratista proporcionará mantenimiento y actualizaciones continuas al servicio de SOC,para asegurar que esté actualizado y protegiendo adecuadamente la infraestructura de la Aerocivil.
- Informes y métricas: El contratista proporcionará informes y métricas ajustadas regulares sobre el rendimiento y la efectividad del servicio de SOC, de acuerdo con los requerimientos del supervisor del contrato.

3.2.2 Inicio del contrato

81. Con la firma del acta de inicio la Aerocivil realizará la entrega de los documentos técnicos, inventarios (de equipos, dispositivos y suscripciones), instructivos, procedimientos, base de conocimiento y demás, y así mismo dispondrá del personal técnico para la implementación del SOC.

82. El contratista se compromete a entregar dentro de los primeros cinco (5) días hábiles posterior a la firma del acta de inicio, un plan detallado para la implementación y puesta en funcionamiento del servicio SOC con los equipos y solución tecnológica de seguridad integrados al SIEM y las herramientas de Ciberseguridad a implementar. La entidad y el contratista deben ajustar y aprobar en dos (2) días hábiles el plan detallado. Y la subsecuente implementación del plan no debe exceder de 30 días calendario garantizando la disponibilidad y disposición de los administradores de las plataformas que serán objeto del servicio, previa revisión y aprobación por el supervisor del contrato designado por la Aerocivil. Durante esos 30 días el contratista debe:

- ❖ En un tiempo no mayor a diez (10) días calendario posteriores de la aprobación, el contratista debe entregar el Plan de Comunicaciones detallado que también debe ser aprobado por el supervisor del contrato. En el plan incluye:
  - Los diversos informes por presentar durante la ejecución del contrato (indicando la finalidad, uso y frecuencia del informe)
  - Los tableros de control a ser implementados (indicando finalidad, uso, oportunidad del control y los niveles de aceptación de los ANS asociados al control, así como sus factores de compensación).
  - Lla matriz de asignación de responsabilidades (RACI) para cada uno de los servicios a prestar.

- ❖ En un tiempo no mayor a quince (15) días calendario posteriores de la aprobación, el contratista debe entregar la matriz de riesgos presentada por la Entidad con su correspondiente Plan de Tratamiento de Riesgos, que debe contener:
  - Los riesgos definidos en la etapa precontractual, contractual y post contractual con los elementos que inciden en la debida ejecución del contrato y de los servicios derivados de éste
  - Esta matriz y el plan debe ser actualizado y se debe realizar seguimiento de manera semestral por parte del contratista.

- Todas las matrices y planes de tratamiento serán acordados entre las partes y debe ser aprobado por el supervisor del contrato o por quien él designe.

❖ En un tiempo no mayor a veinte (20) días calendario posteriores de la aprobación, el contratista debe presentar para aprobación del supervisor, el conjunto de instrumentos e indicadores que permitirán hacer seguimiento a la gestión de cada componente, con sus respectivas desagregación y agregaciones, incluyendo la estructura de documentos, formatos y plantillas, así como cualquier otro instrumento que estime conveniente.

❖ En un tiempo no mayor a treinta (30) días calendario posteriores de la aprobación, el contratista debe implementar los tableros de control y del conjunto de herramientas tecnológicas que lo soportan, en caso, que la implementación de alguna de las herramientas contratadas superen el tiempo establecido el contratista puede entregar un plan de entrega de pendientes que no supere los cuanrenta y cinco (45) días calendario después de la aprobación del plan de implementación (dando quince (15) días calendario adicionales para implementación y puesta en operación). Si supera esos días establecidos se aplicarán los descuentos pertinentes de disponibilidad de las herramientas.

83. La entrega y facturación de los servicios se hará una vez estén implementados y aprobados por el supervisor la totalidad de los componentes técnicos (plataforma), soluciones, funcionalidades, documentos, accesos y demás aspectos (que estén por dentro del alcance del contrato) que requiera la Aerocivil.

3.2.3 Ejecución del contrato y prestación del servicio SOC

84. El contratista debe conocer, adoptar, implementar y en los casos que sea necesario, enriquecer los procesos y procedimientos, actuales, con los que cuenta la Secretaria TI de la Aerocivil con relación a la gestión de eventos cibernéticos y la gestión de seguridad de la información.

85. El contratista debe documentar permanentemente los marcos, modelos, procesos y procedimientos según los parámetros emanados del Sistema de Gestión de Calidad de la Aerocivil, los elementos documentados serán propiedad de la Aerocivil.

86. La documentación sobre la ejecución del contrato se realizará a través de los instrumentos registrados en el formato y/o acordados entre las partes durante el contrato. Para el desarrollo de las etapas anteriormente descritas el contratista debe tener en cuenta las siguientes condiciones:

- El contratista debe definir y contar con el equipo humano de base capacitado y acorde con el objeto contractual, el cual permanecerá en las instalaciones propias del contratista.
- La definición de los marcos, modelos, procesos y procedimientos, así como los instrumentos de seguimiento a la gestión y tableros de control, que se deriven del cumplimiento de los requisitos expuestos en objeto contractual y sus anexos técnicos, deben ser propuestos y dispuestos por el contratista y aprobados por el supervisor, los cuales se considerarán propiedad de la Aeronáutica Civil de Colombia.
- El contratista debe monitorear el inventario tecnológico de la Aeronáutica Civil de Colombia acordado en al alcance del contrato.
- La gestión de eventos, incidentes, problemas y requerimientos/peticiones/solicitudes, debe hacerse usando la herramienta de gestión de la AEROCIVIL en todos los niveles de atención para garantizar un funcionamiento futuro del sistema en el momento de la entrega del servicio finalizando el contrato.
- El contratista debe contemplar una bolsa de 200 horas para ser consumidas en no solo en situaciones post incidentes sino en otro tipo de servicios, como los mencionados de difícil solución, en los cuales el contratista debe acompañar a la Aeronáutica Civil de Colombia en la solución de dichas situaciones.

87. Para el adecuado control y seguimiento de la ejecución del proyecto, la supervisión y la gerencia del proyecto, el contratista y la entidad deben se realizar periódicamente comités de seguimiento, en los cuales se revisará y validará el estado de cumplimiento de las metas del proyecto, y cualquier otra revisión

para la correcta ejecución del proyecto. Estas reuniones deberán tener su correspondiente informe que cumpla con las obligaciones registradas en el presente documento formato 8 Especificaciones Técnicas.

3.2.3.1 Acuerdos de niveles de servicio y factores de compensación de servicios

88. Dentro de la gestión, el Contratista debe implementar una estrategia de control de los ANS en cada una de las líneas de servicio. Este instrumento de seguimiento debe contar con métrica que permita la revisión periódica al supervisor del contrato y/o al equipo que este designe.

89. El propósito del ANS es asegurar la calidad del servicio propuesto por el contratista. Así mismo, el contratista debe hacer uso de los resultados de los ANS's para mejorar el servicio brindado. La validación de los ANS se debe evidenciar en el Dashboard entregado para el servicio, con el cual se evaluará el incumplimiento y sus soportes.

90. El contratista debe administrar los servicios, empleando las mejores prácticas con la finalidad de lograr el cumplimiento de los ANS's y una satisfacción comprobada por la Entidad. El nivel de satisfacción y los mecanismos de medición se establecerán dependiendo de cada indicador.

91. El contratista debe dar cumplimiento de los siguientes ANS's, y para la definición de los Acuerdos de Niveles de Servicio se establece:

- **Incidente:** Cualquier evento que afecte la Confidencialidad, Integridad o disponibilidad de la información o los sistemas que la manejan.
- **Amenaza**: cualquier evento, proceso o actividad que tiene el potencial de causar daño o perjuicio a los sistemas o activos de información de la Aeronáutica Civil de Colombia.
- **Requerimientos**: Son aquellas situaciones reportadas por los usuarios la Aeronáutica Civil de Colombia, o detectados dentro de la operación de los servicios tecnológicos, que no comprometen la disponibilidad de los servicios tecnológicos de la Aeronáutica Civil de Colombia.
- **Prioridad Alta (incidentes)**: Compromete la disponibilidad de los servicios tecnológicos de la Aeronáutica Civil de Colombia, además de los establecidos en las Generalidades del Servicio.
- **Prioridad Media (Incidentes):** Los servicios tecnológicos de la Aeronáutica Civil de Colombia funcionan intermitente, retrasando el normal desarrollo de las actividades cotidianas de los usuarios
- **Prioridad Baja:** Requerimientos relacionadas con las funcionalidades y posibles mejoras de los servicios tecnológicos de la Aeronáutica Civil de Colombia.
- **Tiempo de atención acordado:** Al principio del contrato el contratista y la entidad hará una tabla de tiempos de atención que serán la base de atención acordada durante el contrato.

ACUERDOS DE NIVEL DE SERVICIOS (ANS)								
NOMBRE	**DESCRIPCIÓN/CONDICIÓN**	**UNIDAD DE MEDIDA**	**PERIODO MEDICIÓN**	**META**	**PESO**	**RANGO**	**DESCUENTO MENSUAL**	**CÁLCULO FORMAL**
Gestión de Incidentes: Eficiencia atención de incidentes (Formato 7 item	Hace referencia a la cantidad de incidentes que fueron atendidos dentro del tiempo de atención acordado sobre el total de incidentes	Porcentaje	Mensual	≥95%	10%	Entre 90% - 94,9%	10%	Total de incidentes atendidos dentro del tiempo de atención acordado / Total de incidentes registrados
						Entre 85% - 89,9%	30%	
						Menos de 85%	50%	

2.2)								
Gestión de Requerimientos: Eficiencia solución de requerimientos (Formato 7 item 2.3)	Hace referencia a la cantidad de requerimientos que fueron atendidosdentro del tiempo de atención acordado sobre el total de los requerimientos	Porcentaje	Mensual	≥96%	8%	Entre 90% - 95,9%	10%	Total de requerimientos atendidos dentro del tiempo de atención acordado / Total de requerimientos registrados
						Entre 85% - 89,9%	30%	
						Menos de 85%	50%	
Porcentaje de incidentes reabiertos y su efectividad. (Formato 7 item 2.2)	Hace referencia al porcentaje de casosreabiertos después de ser atendidos y cerrados. Este indicador no debe superar el 2% del total de los servicios atendidos durante el mes.	Porcentaje	Mensual	≤2%	5%	Mayor a 2%	10%	1. Total de incidentesreabiertos / total de incidentes atendidos
Porcentaje de requerimientos reabiertos y su efectividad. (Formato 7 item 2.3)	Hace referencia al porcentaje de casosreabiertos después de ser atendidos y cerrados. Este indicador no debe superar el 2% del total de los servicios atendidos durante el mes.	Porcentaje	Mensual	≤2%	5%	Mayor a 2%	10%	2. Total de incidentesreabiertos / total de incidentes atendidos 3. Total de requerimientos reabiertos / total de requerimientos atendidos
Disponibilidad de las herramientas de monitoreo SOC (Formato 7 item 2.1)	Entendida como el normal funcionamiento de la herramienta demonitoreo SOC	Porcentaje	Mensual	≥99,5%	10%	Entre 94,5% - 99,4%	10%	(Hora Mes - Horas Manto. programado - Horas indisponibles) / (Horas mes - Horas Manto. programado)
						Entre 89,6% - 94,5%	30%	
						Menos de 89,5%	50%	
						Entre 89,6% - 94,5%	30%	
						Menos de 89,5%	50%	
						Entre 99% - 89%	15%	
						Entre 89% - 79%	30%	

						Entre 79% - 69%	45%
						Entre 69% - 50%	60%
						Menos de 50%	100%

NOTA 1: Los tiempos medidos para la disponibilidad de herramientas tipo SOC serán tenidos en cuenta siempre y cuando la falla se presente sobre las plataformas prestadores del servicio SOC, no se hará efectivo en el caso de falla de canales de conectividad y/o plataformas o herramientas fuera del alcance del SOC. Para determinar ello se debe generar un reporte por parte del equipo SOC donde se evidencia que la falla está relacionada por sus responsabilidades.

NOTA 2: En caso de presentarse, tiempos adicionales de solución por actividades propias en el componente afectado, como ventanas de mantenimiento, configuraciones, aplicación de parches, estos deben ser incluidos, con la explicación y justificación respectiva, en el plan de trabajo presentado al Comité de Cambios en donde se evaluará también la eventualidad para el cumplimiento del ANS.

92. Por servicios no prestados en las condiciones exigidas y asociadas al servicio SOC responsabilidad del contratista, se realizará un descuento directo a la factura del servicio, previa revisión y aprobación mediante acta firmada por el Supervisor del Contrato Representante legal y Gerente del Proyecto por parte del contratista.

3.2.3.2 Visitas de campo

93. Es responsabilidad del Contratista presentar el cronograma de las visitas que sean necesarias en la Institución, para recopilar la información requerida, que supla las necesidades del proyecto, y visitas adicionales para la prestación de los servicios de SOC.

94. El contratista debe comunicar y coordinar con un tiempo prudente, no menor a diez (10) días de anticipación la solicitud de permisos para las visitas y trabajos a realizar dentro de las instalaciones de la Institución, deben, asimismo, cumplir con los requerimientos establecidos por la Institución para su ingreso a realizar actividades en sus instalaciones.

95. El contratista debe asumir por su cuenta los costos que sean necesarios para las visitas y trabajos a realizar en las instalaciones de la Institución objeto de este contrato, estos costos el consultor los deben contemplar e incluirlos dentro de cada uno de los entregables establecidos en el formato económico del pliego, no es responsabilidad de la Institución ningún reproceso o logística necesaria por parte del contratista por falta de planeación, y la Institución no responderá por ningún sobre costo en logística que no se haya contemplado por el contratista.

96. Es responsabilidad del contratista cumplir con todos los protocolos de Seguridad, Bioseguridad y Administrativos para el ingreso a las instalaciones de la Institución, es responsabilidad del contratista si, su personal realiza alguna afectación a equipos u operación dentro las instalaciones de la Institución en su etapa de recolección de información a las instalaciones el cual debe responder económicamente y moral por la acción efectuada.

97. La Entidad podrá solicitar las mesas de trabajo a los expertos que considere necesarios para hacer debates técnicos para el bien del proyecto, estos costos el contratista los debe tener en cuenta dentro de su evaluación económica de la propuesta y ser incluidos en cada uno de los entregables del proyecto.

3.2.3.3 Mesas de trabajo entre contratista, entidad y stakeholders

98. Es obligación del Contratista gestionar y coordinar la logística correspondiente al desarrollo y ejecución de las actividades contractuales pactadas, incluyendo:
    - ❖ Presentación del cronograma general de mesas de trabajo.
    - ❖ Programación respectiva con las partes interesadas o stakeholders que requiere para el desarrollo de la ejecución de los trabajos asociados al servicio de SOC.

99. El Contratista junto con la supervisión designada por la Institución debe programar las mesas de trabajo, tanto las iniciales, de desarrollo por fase de avance del proyecto y la final, con el fin de articular la información, con la que ya se cuente en la Entidad en todo lo relacionado con el monitoreo de los incidentes cibernéticos de la infraestructura actual de TI de la Institución.

100. Así mismo, es obligación del Contratista la asistencia y participación de forma física presencial por parte del equipo de trabajo aprobado por la Institución para la ejecución del proyecto, en el lugar del contrato y dejar registro escrito y fotográfico de todas las reuniones realizadas con cualquier tipo de actor que intervenga en el desarrollo de la prestación de los servicios de SOC.

3.2.4 Cierre del contrato y finalización de la prestación del servicio SOC

101. Al finalizar la ejecución del contrato, el contratista hará entrega formal al supervisor del contrato, de todos los informes, documentación histórica, equipos y software a que haya lugar y toda la base del conocimiento e información técnica en su última versión y la información que el supervisor del contrato solicite con respecto al desarrollo del contrato.

102. Por otro lado, dentro de los sesenta (60) días anteriores a la finalización del contrato, el contratista debe presentar el plan detallado del cierre y entrega de los servicios contratados.

103. Así mismo, un (1) mes antes a la terminación del contrato, el Contratista debe realizar un empalme, capacitación y transferencia de conocimiento al supervisor del contrato o a máximo 2 personas quien este designe.

104. Todo lo anterior debe ser aprobado previamente por el supervisor del contrato antes de comenzar la fase de cierre.

Nota 1: Los costos asociados a esta etapa de entrega de los servicios a la Aerocivil deben estar contemplados en los costos unitarios del equipo base mínimo para ejecutar el servicio, por lo que no se generarán costos adicionales para la Entidad.

4. GARANTÍA TÉCNICA

- El contratista se obliga a dar cumplimiento a las disposiciones establecidas en los artículos 932 y 933 del Código de Comercio, Ley 1480 de 2011, Decreto 735 de 2013 y demás normas que lo modifiquen o adicionen.
- Actividad que se desarrollará luego de la implementación del servicio y durante la ejecución del contrato.
- La garantía no debe generar costos adicionales para la Entidad y aplica para todos los servicios suministrados.
- El contratista debe responsabilizarse por los problemas o deficiencias técnicas que se presenten durante la ejecución del contrato.
- La Entidad a través del supervisor del contrato informará de manera inmediata la generación de cualquier falla o degradación del servicio presentada, como consecuencia de la implementación y prestación del servicio objeto del presente proceso de contratación; este reporte se realizará vía telefónica o al correo electrónico informado por el contratista.
- Todos los costos en que se deba incurrir para garantizar el correcto funcionamiento del servicio suministrado e implementado objeto del presente contrato estarán a cargo del contratista y deben contemplarse dentro de su propuesta económica.

5. ANEXO 1 : INVENTARIO DE ACTIVOS DE TI.

INVENTARIO GENERAL PLATAFORMA TECNOLÓGICA		
La infraestructura de la Aeronáutica Civil en la actualidad está compuesta de 35 servidores físicos, 152 servidores virtuales, 30 BD Oracle Producción, 18 BD Oracle pruebas, 2 sistemas de almacenamiento SAN, 2 switche Core Cisco, 350 switches multivendor, 2 Balanceadores de carga, 2 Esxi 7.0.3 1, 60 Firewall Fortinet, Protección Endpoint XDR Fortinet (1 por cada computador y servidor), WAF- Cloud Fortinet, 1 Fortianalyzer Fortinet, correo electrónico suite Microsoft 365 (4000 buzones aprox)		
Infraestructura	Sistemas Operativos Servidores	• 9 Servidores Linux SUN-DELL Redhat 6.10 • 2 Servidores Linux SUN Redhat 5.11 • 2 Servidores Linux SUN Redhat 5.11 • 2 Servidores Linux DELL Redhat 7.6 • 1 Servidor Linux VMware, Inc. Redhat 8.1 • 2 Servidores Linux VMware, Inc. Redhat 8.2 • 1 Servidor Linux VMware, Inc. Redhat 8.4 • 4 Servidores Linux DELL-VMWARE Redhat 8.5 • **6 Servidores Windows Microsoft Windows Server 2008 R2 Enterprise (1)** • **34 Servidores WindowsMicrosoft Windows Server 2012 R2 Standard (1)** • 27 Servidores Windows Microsoft Windows Server 2016 Datacenter • 12 Servidores WindowsMicrosoft Windows Server 2016 Standard • 21 Servidores Windows Microsoft Windows Server 2019 Datacenter • 25 Servidores WindowsMicrosoft Windows Server 2019 Standard
	Sistemas Operativos Estaciones de trabajo	• 1143 PC usuarios Microsoft Windows 10 Enterprise • 1326 PC usuarios Microsoft Windows 10 Pro • 5 PC usuarios Microsoft Windows 10 Pro for Workstations • 25 PC usuarios Microsoft Windows 11 Enterprise • 16 PC usuarios Microsoft Windows 11 Pro • 1 PC usuario Microsoft Windows 7 Professional • 84 PC usuarios Microsoft Windows 8.1 Pro

	Bases de datos	• 9 Oracle Database Versions: 11.2.0.3.0 • 4 Oracle Database Versions: 12.1.0.2.0 • 35 Oracle Database Versions:12.1.0.1.0

	Firewall y equipos core de seguridad informática	Firewall	Fortigate	61F
		Firewall	Fortigate	91G
		Firewall	Fortigate	1000F
		• Los Firewall Fortinet tiene integración SD-WAN, adicionalmente configurado las siguientes características: Antivirus, WAF- cloud, Web Filter, DNS Filter y Application Control.		
	Servicios de seguridad de la información	• XDR de Fortinet cuenta con la tecnología de inteligencia artificial y de aprendizaje automático para detectar técnicas de malware, ransomware, phishing, kits de explotación.		

Datos adicionales:

- Cantidad de IPs internas, externas y URLs a ser monitoreadas
  - IPs internas 500 escalables a 700 criticas.
  - IPs externas 50 escalable a 128.
  - URLs: 17 escalable a 25.
- Cantidad de Activos monitoreados SOC: 700 escalable hasta 900
  - Activos críticos: 300 escalable hasta 500
  - Activos Críticos con Agentes Avanzados: 400
- Cantidad de usuarios de alto riesgo para la organización monitoreados SOC:
  - Usuarios Estaciones de Trabajo: 2700 escalable a 3500
  - Usuarios Directorio Activo: 400
  - Usuarios Correo Electrónico O365: 500
- Gestión de Vulnerabilidades:
  - Activos Infraestructura interna: 400 escalable hasta 500
  - Aplicaciones Web: 5
- Cantidad de Activos monitoreados Performance - NOC: 500
  - Activos críticos: 500

(1) En proceso de migración y actualización y deben ser monitoreados cuando la opción esté disponible

6. ANEXO 2: ABREVIATURAS Y DEFINICIONES

A continuación, se enuncian algunas abreviaturas y definiciones, las cuales se utilizarán en los anexos técnicos y son la representación escrita de una palabra con una o varias de sus letras:

6.1.1 ABREVIATURAS

- Aerocivil: Aeronáutica Civil de Colombia.
- ANS: Acuerdos de Nivel de Servicio.
- ITIL: Conjunto de conceptos y buenas prácticas usadas para gestionar servicios de tecnologías de la información, desarrollar tecnologías de la información y operaciones relacionadas con esta.
- PETI: Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
- PMBOK: La guía del PMBOK es un instrumento desarrollado por el Project Management Institute (o PMI), que establece un criterio de buenas prácticas relacionadas con la gestión, la administración y la dirección de proyectos.
- TI: Tecnologías de la Información.
- TO: Tecnologías de Operación
- TIC: Tecnologías de la Información y Comunicación.
- SI: sistemas de Información
- DDOs: (Distributed Denial of Service): es un tipo de ataque cibernético en el que múltiples dispositivos comprometidos seutilizan para inundar un servidor o una red con tráfico malintencionado, lo que resulta en la interrupción o la denegación deservicio para los usuarios legítimos.
- SOC (Security Operations Center): Security Operations Center es una instalación que centraliza la monitorización y gestión de la seguridad de la información de una organización.
- NOC (Network Operations Center): Centro de Operaciones de Red. Un NOC es una instalación que centraliza la monitorización, gestión y mantenimiento de la red de una organización.
- SIEM: Security Information and Event Manager:es una solución de seguridad que combina la funcionalidad de dos tipos deherramientas de seguridad: la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM).
- VPN: significa "Virtual Private Network" (Red Privada Virtual, en español) y se refiere a una tecnología de red que permite crear una conexión segura y privada a través de una red pública como Internet.
- DMZ significa "zona desmilitarizada" (del inglés "demilitarized zone"). Una red intermedia entre la red interna de una organización y la red externa (generalmente Internet), utilizada para alojar servicios y recursos disponibles para el público, pero protegidos de posibles ataques externos.

6.1.2 DEFINICIONES

- ACCESO: La puesta a disposición por parte de un proveedor a otro proveedor, de recursos físicos y/o lógicos de su red para la provisión de servicios. El acceso implica el uso de las redes.
- ACTIVIDADES: Son el conjunto de operaciones mediante los cuales se genera valor al utilizar los insumos, dando lugar a un producto determinado.
- APLICACIONES: Son programas de computador que están diseñados con capacidades lógicas y matemáticas para procesar información. El término Aplicación se utiliza para agrupar un conjunto de programas que responden a requerimientos particulares del negocio o área de negocio.
- ACUERDO DE NIVEL DE SERVICIO (ANS): Es un convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.[1]
- ARQUITECTURA: Según ISO/IEC 42010: Proceso de concebir, expresar, documentar, comunicar, certificar la implementación, mantener y mejorar la

arquitectura a través de todo el ciclo de vida de un sistema.[2]

- ARQUITECTURA DE SISTEMAS DE INFORMACIÓN: Incluye la descripción detallada de cada una de los sistemas de información y las relaciones entre ellos. Cada sistema de información debe contar con una ficha técnica que los describa. Esta dimensión debe hacer el enlace entre la Arquitectura de Negocio y la visión de TI.[3]
  ARQUITECTURA DE SERVICIOS TECNOLÓGICOS: La arquitectura de servicios tecnológicos o infraestructura incluye todos los elementos de TI que soportan la operación de la entidad. En esta dimensión se va desde la plataforma de hardware y de comunicaciones, hasta el software especializado que permite soportar las arquitecturas de información y de sistemas deinformación.[4]
- ACTIVO: Cualquier cosa que tiene valor para la organización, NTC-ISO /IEC 27001.
- ANÁLISIS DE RIESGO: Uso sistemático de la información para identificar las fuentes y estimar el riesgo, NTC-ISO /IEC 27001.
- AUDITORIA: proceso de evaluación y revisión de los sistemas informáticos, infraestructuras de tecnología de la información y procesos de negocio para determinar su eficiencia, seguridad y cumplimiento normativo.
- AUTENTICACION: proceso de verificar la identidad de un usuario que intenta acceder a un sistema o recurso en línea.
- BASE DE CONOCIMIENTO: Portafolio de instrumentos y herramientas que guían y ayudan a la implementación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.[5]
- BLUE TEAM: grupo de profesionales de seguridad informática que trabajan en la defensa de una organización contra ataques cibernéticos. Los profesionales del Blue Team se enfocan en mantener la seguridad de la red y en prevenir y detectar ataques.
- CALIDAD DE SERVICIO (QOS): El efecto global de la calidad de funcionamiento de un servicio que determina el grado de
- COMPONENTE DE TI: Hace referencia a cualquier elemento de TI (software, hardware o componente de información) de una institución, lo mismo que a sus procesos, capacidades y servicios.[6]
- CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- CORE: Elemento que corresponde a la parte o función principal de algo. En Informática es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.
- CRIPTOGRAFIA: es una técnica de seguridad que se utiliza para proteger la información mediante la transformación de los datos originales en un formato ilegible llamado cifrado
- DATACENTER: Es una instalación física utilizada para alojar servidores, sistemas de almacenamiento y otros componentes de infraestructura de tecnología de la información (TI).
- DATO: Es una representación simbólica de una característica particular de un elemento o situación, que pertenece a unmodelo de una realidad. Tiene un tipo (por ejemplo, numérico, cadena de caracteres o lógico) que determina el conjunto de valores que el dato puede tomar. En el contexto informático, los datos se almacenan, procesan y comunican usando medios electrónicos. Constituyen los elementos primarios de los sistemas de información.[7]
- DATOS ABIERTOS: Son los datos primarios (sin procesar) en formatos estándar e interoperables que facilitan su acceso y reutilización, que están bajo la custodia de las entidades públicas y que se ponen a disposición de cualquier ciudadano, libre y sin restricciones, para que terceros puedan reutilizarlos y crear servicios derivados de estos. Las principales características de los datos abiertos son:

  - **Completos:** Los datos públicos no deben estar sujetos a privacidad u otras limitaciones. Además, deben estar electrónicamente almacenados.
  - **Primarios:** Significa que debe haber una disponibilidad de la fuente primaria, sin procesamientos y sin formas agregadas.
  - **Oportunos:** Ello para preservar su valor.
  - **Accesibles:** La disponibilidad debe ser lo más amplia posible para los usuarios y para propósitos diversos.
  - **Procesables:** Deben estar razonablemente estructurados para permitir su automatización por diversas herramientas.
  - **Acceso indiscriminado:** Implica su disponibilidad para cualquier usuario, sin necesidad de su registro.
  - **No-propietarios:** Deben estar disponibles en un formato donde nadie deba tener la exclusividad de su control.

- **Libres de licencias:** No deben estar sujetos a copyright, patentes, o regulaciones secretas. Una razonable privacidad, seguridad y restricciones puede ser aplicada por el gobierno u otros estamentos.[8]

- DEVOPS: DevOps es un conjunto de prácticas que agrupan el desarrollo de software y las operaciones de TI. Su objetivo es hacer más rápido el ciclo de vida del desarrollo de software y proporcionar una entrega continua de alta calidad.
- DISPONIBILIDAD: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.
- DOMINIO: Cada uno de los seis componentes que conforman la estructura de la primera capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial para la gestión de TI. Los dominios son las dimensiones desde las cuales se debe abordar la gestión estratégica de TI. Agrupan y organizan los objetivos, áreas y temáticas relativas a las TI.[9]
- ELEMENTO: Tema de relevancia que se destaca dentro de cada ámbito.[10]
- ENTORNO DIGITAL: Ambiente físico y virtual sobre el que se soporta la economía digital. Siendo esta última la economíabasada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.[11]
- ESTÁNDARES: En el contexto de TI, un estándar es un documento que contiene un conjunto de especificaciones técnicas de aplicación voluntaria, que ha sido construido a través de consenso y que refleja la experiencia y las mejores prácticas en un área en particular.[12]
- ESTRATEGIA TI: Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en que una entidad utiliza las Tecnologías de la Información para lograr su misión de manera eficaz. La Estrategia TI es una parte integral de la estrategiade una entidad.[13]
- EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar laimportancia del riesgo.[14]
- EVENTO: se refiere a cualquier suceso que se produce en un sistema o red informática y que puede ser registrado o monitoreado.
- FIREWALL: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.[15]
- FLUJO DE INFORMACIÓN: Corresponde a la descripción explicita de la interacción entre proveedores y consumidores deinformación, con un patrón repetible de invocación definido por parte de la entidad. Puede incorporar servicios de información, datos e información.[16]
- FUNCIÓN: Responsabilidad o actividad inherente a un rol.[17]
- GESTIÓN TI: Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.[18]
- GOBERNABILIDAD: Define la capacidad de una organización para controlar y regular su propio funcionamiento con el fin de evitar los conflictos de intereses relacionados con la división entre los beneficiarios y los actores[19].
- INCIDENTE DE SEGURIDAD: evento no planificado que involucra la pérdida, divulgación no autorizada, alteración o destrucción de información o sistemas de información.
- HERRAMIENTAS: Mecanismos que les permiten a las instituciones materializar acciones específicas asociadas con directrices dadas por el Marco de Referencia de Arquitectura Empresarial para la Gestión TI, específicamente por un lineamiento o una guía. Las herramientas son identificadas y referenciadas con base en las mejoras prácticas de TI para apoyar la arquitectura y la gestión.[20]
- INDICADOR: En el contexto de la informática, un indicador es una medida de logro de algún objetivo planteado.[21]
- INFORMACIÓN: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.[22]
- INSTRUMENTO: Es un medio o recurso que se puede utilizar en el desarrollo de acciones para lograr un resultado deseado. Por ejemplo, guías, especificaciones técnicas, formatos o plantillas, entre otros.[23]
- INTEGRIDAD: Propiedad de salvaguardar la exactitud y completitud de la información y asegurar que sus métodos de procesamiento sean exactos.
- INTEROPERABILIDAD: Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información.

(Gobierno de Australia). Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. (ISO). Colaborar organizaciones para intercambiar información y conocimiento en sus procesos de negocio, para facilitar la entrega de servicios en línea a ciudadanos, empresas y otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010).[24]

- IPv6: El Protocolo de Internet versión 6, es la versión del Protocolo de Internet (IP por sus siglas en inglés) que fue diseñada para suceder al Protocolo versión 4. Ipv6 ha sido desarrollado por la Internet Engineering Task Force (IETF -www.ietf.org), para hacer frente al agotamiento de las direcciones Ipv4, y se describe en el documento estándar de Internet RFC 2460, publicado en diciembre de 1998. Aunque Ipv4 de 32 bits permite una dirección de Protocolo de Internet, y por lo tanto puede soportar232 direcciones, Ipv6 utiliza direcciones de 128 bits, por lo que el nuevo espacio de direcciones compatible con 2128. Estaexpansión permite muchos más dispositivos y usuarios en Internet, así como una mayor flexibilidad en la asignación de direcciones y la eficiencia para el direccionamiento de tráfico.[25]
- ISO27001: Esta norma es un estándar para la seguridad de la información emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2022 y ahora su nombre completo es ISO/IEC 27001:2022.[26]
- LINEAMIENTO: Es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano.[27]
- MADUREZ: Indica el grado de confiabilidad que el negocio puede tener en un proceso, gracias a la capacidad de este para alcanzar las metas y objetivos deseados.
- MATRIZ RACI: Es una herramienta de gestión de proyectos que se utiliza para definir y comunicar roles y responsabilidades en un proyecto. La matriz RACI establece las responsabilidades de las personas y/o equipos involucrados en un proyecto y ayuda a evitar confusiones y superposiciones en las tareas y responsabilidades.
- MESA DE SERVICIO: Es una unidad funcional dedicada a gestionar una variedad de eventos sobre el servicio. La mesa puede ser un punto único de contacto para los usuarios de TI. Maneja los incidentes y solicitudes de servicio a través del uso deherramientas especializadas para dejar registro y administrar los eventos.[28]
- MEDIDAS CORRECTIVAS: acciones que se toman para corregir o remediar los problemas de seguridad de la información que han sido identificados. Estas medidas pueden ser implementadas después de que se ha producido un incidente de seguridad o después de la identificación de una vulnerabilidad o debilidad en el sistema de seguridad
- MEDIDAS PREVENTIVAS: acciones que se toman para evitar o reducir el riesgo de incidentes de seguridad de la información. Estas medidas se implementan antes de que ocurra un incidente para reducir las posibilidades de que se produzcan, o para minimizar su impacto en caso de que ocurran.
- META: Dentro de un modelo estratégico, los objetivos se detallan a través de metas, las cuales definen de manera cuantitativa el logro esperado en un aspecto específico. El objetivo se cumple cuando todas sus metas se logran. Una meta debe serprecisa y medible a través de indicadores.[29]
- NIST: es una serie de estándares y guías publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, que aborda diversos aspectos de la seguridad de la información, incluyendo la gestión de riesgos, la ciberseguridad, la privacidad, entre otros. La norma NIST proporciona un marco de referencia para la implementación de medidas de seguridad de la información, y se utiliza ampliamente en todo el mundo por organizaciones públicas y privadas, así como por gobiernos y agencias gubernamentales. El marco de referencia de la norma NIST está compuesto por varias publicaciones, siendo las más conocidas y utilizadas el "Framework para la Mejora de la Ciberseguridad" (NIST CSF) y el "Marco de Gestión de Riesgos de Ciberseguridad" (NIST RMF). El NIST CSF es una guía que ayuda a las organizaciones a evaluar y mejorar su postura de seguridad de la información, mientras que el NIST RMF es un marco para la gestión de riesgos de seguridad de la información que ayuda a las organizaciones a identificar, evaluar y mitigar los riesgos de seguridad de la información.
- NORMATIVIDAD: Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
- NUBE: La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.[30]
- ON-PREMISE: La infraestructura tecnológica on-premise se refiere a los componentes físicos y lógicos de tecnología que se encuentran instalados y operan en las instalaciones de la organización. Estos componentes pueden incluir servidores, sistemas de almacenamiento, dispositivos de red, software de gestión

de sistemas, entre otros.

- OFIMÁTICA: Herramientas de oficina usadas en las entidades como lo son hojas de cálculo, procesamiento de texto, entre otros.[31]
- POLÍTICA DE TI: Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Las políticas son usadas para dirigir las decisiones, para asegurar la consistencia y el apropiado desarrollo e implementación de los procesos, estándares, roles, actividades y servicios de TI.
- PMI (Project Management Institute): El Instituto fue fundado como una asociación de miembros autónoma, sin fines de lucro, dedicada a hacer avanzar el estado del arte en la efectiva y apropiada aplicación de la práctica y la ciencia de la Dirección de Proyectos.[32]
  PETI (o PETIC por sus siglas): El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Cada vez que una entidad hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.[33]
- PLAN DE CAPACITACIÓN Y ENTRENAMIENTO: Define las actividades de capacitación y entrenamiento que se requieren para entrenar a los funcionarios de una entidad en aspectos específicos de una aplicación, una metodología, un producto, una tecnología o un proceso.[34]
- PLATAFORMA SIEM: SIEM (Security Information and Event Management) conjunto de tecnologías y procesos utilizados para gestionar eventos de seguridad y monitorizar la seguridad de la información en el MINTIC.
- PLUGIN**:** Un plugin es un componente de software que se agrega a una aplicación o plataforma para proporcionar una funcionalidad adicional. Los plugins suelen ser pequeñas piezas de software que se integran con la aplicación principal y se ejecutan dentro de ella.
- RED**:** conjunto de dispositivos interconectados entre sí que se comunican y comparten recursos entre sí. Estos dispositivos pueden ser computadoras, servidores, dispositivos móviles, enrutadores, switches, entre otros**.**
- RIESGO El riesgo es el efecto de la incertidumbre sobre los objetivos.[35]
- RIESGO DE SEGURIDAD: se refiere a la posibilidad de que un evento adverso o una amenaza potencial se materialice ycause daños o pérdidas en los sistemas o activos de una organización. Estos riesgos pueden ser internos o externos y pueden incluir amenazas como ciberataques, errores humanos, fallos en el sistema, desastres naturales, entre otros.
- RED TEAM: Es un grupo de profesionales de seguridad informática que trabajan para evaluar la seguridad de una organización mediante la simulación de ataques cibernéticos. El objetivo principal del equipo Red Team es detectar y explotar vulnerabilidades en la red y los sistemas de una organización, de manera similar a cómo lo harían los atacantes reales.
- ROLES: Conjunto de responsabilidades y actividades asignadas a una persona o grupo de personas para apoyar la adopción y aplicación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.[36]
- SEGURIDAD DE LA INFORMACION: es el conjunto de prácticas, tecnologías y políticas que se utilizan para proteger la confidencialidad, integridad y disponibilidad de la información.
- SEGURIDAD PERIMETRAL: conjunto de medidas y tecnologías diseñadas para proteger la red y los sistemas del MINTICdesde el exterior, o sea, desde su perímetro
- SERVICIO: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.[37]
- SERVICIO DE INFORMACIÓN: Consiste en la entrega de información de valor para los usuarios de una entidad a través de un proveedor de servicio interno o externo. Un servicio de información se describe a través de un contrato funcional (qué recibe como entrada y qué produce como salida) y un conjunto de acuerdos de servicio que debe cumplir.[38]
- SERVICIO TECNOLÓGICO: Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos

de calidad como disponibilidad, seguridad, confiabilidad, etc.[39]

- SERVICIO DE TI: Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficienteimplementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los servicios de TI deben tener asociados unos acuerdos de nivel de servicio.[40]
- SERVICIO EN LÍNEA: Servicio que puede ser prestado por medios electrónicos a través del portal de una entidad.[41]
- SERVIDOR: dispositivo o sistema informático que provee servicios a otros dispositivos o sistemas llamados clientes. Estosservicios pueden ser de distintos tipos, como almacenamiento de datos, procesamiento de información, gestión de correoelectrónico, acceso a aplicaciones o servicios web, entre otros.
- SISTEMAS DE INFORMACIÓN: Es un conjunto formal de procesos que, operando con un conjunto estructurado de datos, y de acuerdo con las necesidades de una empresa, recopila, procesa y almacena información necesaria para la operación de dicha empresa y para las actividades de dirección de control correspondientes, apoyando la toma de decisiones necesaria para desempeñar las funciones y procesos de negocio de la empresa de acuerdo con su estrategia.[42]
- STAKEHOLDER: Cualquier grupo o individuo que puede afectar o ser afectado por el logro de los objetivos de la empresa.[43]
- TABLERO DE INDICADORES: Es un conjunto de indicadores cuya medición y seguimiento periódico brindará un mayor conocimiento sobre la situación real de una institución y el avance en el logro de sus objetivos. Un tablero de indicadoresincluye una mezcla de indicadores estratégicos, tácticos y operativos.[44]
- VULNERABILIDAD**:** debilidad o defecto en un sistema o aplicación que puede ser explotado por un atacante para comprometer la seguridad del sistema o la privacidad de los datos. Las vulnerabilidades pueden existir en diferentes componentes del sistema, como software, hardware, redes, sistemas operativos, aplicaciones, y otros.

---

[2] https://gobiernodigital.mintic.gov.co/692/articles-272872_Conceptos_clave_Arquitectura.docx
[3] PETIC-Mintic – diciembre 2022, https://www.minagricultura.gov.co/planeacion-control-gestion/Paginas/Gestion.aspx.
[4] PETIC-Mintic – diciembre 2022,
[5] https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[6] https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[7] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[8] https://www.mintic.gov.co/portal/inicio/Glosario/
[9] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[10] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[11] https://www.mintic.gov.co/portal/inicio/Glosario/
[12] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[13] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[14] NTC-ISO /IEC 27001
[15] https://www.mintic.gov.co/portal/inicio/Glosario/
[16] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[17] https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[18] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[19] PETIC Sectorial. MADR – diciembre 2016,
[20] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[21] Tomado de: http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[22] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html

[23] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[24] https://www.mintic.gov.co/portal/inicio/Glosario/
[25] https://www.mintic.gov.co/portal/inicio/Glosario/
[26] Tomado de https://ingertec.com/nueva-version-iso-27001-2022/
[27] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[28] https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[29] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[30] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[31] https://www.mintic.gov.co/portal/inicio/Glosario/
[32] Tomado de http://repositorio.uchile.cl/tesis/uchile/2007/ec-vasquez_g/pdfAmont/ec-vasquez_g.pdf
[33] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[34] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[35] https://www.mintic.gov.co/portal/inicio/Glosario/
[36] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[37] https://www.mintic.gov.co/portal/inicio/Glosario/
[38] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[39] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[40] Tomado de http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
[41] https://www.mintic.gov.co/portal/inicio/Glosario/
[42] Libro: Desarrollo de sistemas de información: una metodología basada en el modelado, Concepto de Andreu, Ricart y Valor (1996)
[43] http://www.scielo.org.co/pdf/agc/v28n3/v28n3a16.pdf
[44] https://www.ipes.gov.co/images/informes/SDE/Planeacion_estrategica/PLAN%20PETI%202021-2024%20PA08-DE-001%20V2.pdf